Health Compliance Through a Transparent Supply Chain

Primal Wijesekera
International Computer Science Institute (ICSI) & UC Berkeley

***Abstract*—Privacy regimes are increasingly taking center stage for bringing up cases against violators or introducing new regulations to safeguard consumer rights. Health regulations mostly predate most of the generic privacy regulations. However, we still see how health entities fail to meet regulatory requirements. Prior work suggests that third-party code is responsible for a significant portion of these violations. Hence, we propose using Software Bills of Materials (SBOM) as an effective intervention for communicating compliance limitations and expectations surrounding third-party code to help developers make informed decisions.**

***Index Terms*—Mobile Privacy, Compliance, Supply Chain Transparency**

1. Introduction

Prior research has examined different dimensions required for a successful privacy regime: the effectiveness of privacy policies [1], [2], [5], [10], [11], proposals for more usable alternatives [7], [8], [12], preliminary studies on GDPR Data Subject Access Requests (DSARs) [3], [9], etc. To understand the discrepancy between the "law in the books" and the "law in action", examining one of the often overlooked roles the supply chain plays in software development is required.

While there is rich literature on how software systems comply with specific clauses, only recently has the literature looked at the third-party code's impact towards compliance [14]. Prior work found that in responding to *verified consumer requests* under CCPA [4], a statistically significant amount of apps could not respond correctly due to resources accessed by third parties – a clear sign of the negative impact done by third-party code. In another prior work on measuring compliance of COPPA [13] and in health app analysis [6], developers were open to changing their behavior upon receiving information about in-compliant third-party code. It is a sign that if they had prior knowledge, there is a significant chance they would not have embedded that third-party code in their systems. This leads to our hypothesis that we can fix a sizable chunk of compliance issues by creating a more transparent supply chain ecosystem for developers.

We believe there are two orthogonal issues developers face before embedding a third-party code: a) developers are not aware of the nature of the data accessed by third-party code and with whom such sensitive data is shared – this is problematic if the third party shares data with a non-compliant recipient or if a third party accesses a sensitive resource such as location without proper user authorization again violating a regulatory requirement and b) for health data, the issue is a little bit more complex – and which third party library is complying with what regulation is not easily understandable based on the public information.

The principal question is understanding how to convey this compliant info to the developer. Entities such as Facebook and Google are already publicly asking developers not to use their SDKs in regulated domains such as health. However, many apps still use their SDKs to share data, potentially violating regulatory requirements. It raises questions on the effectiveness of public information or the disregard of such information by the developers. Many regulated health entities do not have an internal development team, so they hire outside development entities who may or may not fully understand the ramifications of embedding non-compliant third parties. A clearly defined SBOM will, in this case, help the regulated entity to understand the composition of the software they are going to acquire and the potential legal issues.

A Multi-Stakeholder Focus Group. We intend to hold a focus group understanding the following questions among state and federal regulators, health entities (hospitals, online clinics, insurance organizations), developers of health systems, legal/compliance teams (both internal and externally hired legal teams), CISA SBOM representative and developers from popular SDKs. The key questions we intend to have a deep dive into are:

1) What are the legal expectations of data sharing and receiving in health apps?
2) How would a well-structured SBOM help to meet legal obligations?
3) How would a SBOM affect the legal accountability of health entities and third-party code owners?
4) What are the challenges and factors that could affect implementing a transparent SBOM ecosystem in the health sector?
5) What are the components of a transparent and detailed SBOM in the health sector? How do we correctly express regulatory restrictions?
6) How do third-party code providers perceive an SBOM ecosystem in the health sector?

We expect to produce a draft SBOM with the agreed-upon components for SBOM and a set of processes that the focus group participants suggest to use the SBOM effectively. As a follow-up/validation study, we plan to do

an online survey among privacy practitioners and healthcare experts to understand the wider community's response and opinion.

Acknowledgment

This work was supported by the U.S. National Science Foundation (under grant CNS-2055772).

References

[1] A. Anton, J. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen. Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, 2(2):36–45, Mar-Apr 2004.

[2] R. Böhme and J. Grossklags. The security cost of cheap user interaction. In *Proceedings of the 2011 workshop on New security paradigms workshop*, NSPW '11, pages 67–82, New York, NY, USA, 2011. ACM.

[3] C. Boniface, I. Fouad, N. Bielova, C. Lauradoux, and C. Santos. Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data. In *Proceedings of the Annual Privacy Forum*, 2019. https://www-sop.inria.fr/members/Nataliia.Bielova/papers/Boni-etal-19-APF.pdf.

[4] California Consumer Privacy Act (CCPA). California Civil Code §1798.100 et seq.

[5] J. Earp, A. Anton, L. Aiman-Smith, and W. Stufflebeam. Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2):227–237, May 2005.

[6] M. Huo, M. Bland, and K. Levchenko. All eyes on me: Inside third party trackers' exfiltration of phi from healthcare providers' online systems. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, pages 197–211, 2022.

[7] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA, 2009. Association for Computing Machinery.

[8] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1573–1582, New York, NY, USA, 2010. Association for Computing Machinery.

[9] J. L. Kröger, J. Lindemann, and D. Herrmann. How do app vendors respond to subject access requests? a longitudinal privacy study on ios and android apps. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, 2020. Association for Computing Machinery.

[10] A. McDonald and L. Cranor. The cost of reading privacy policies. In *Proceedings of the Technology Policy Research Conference*, September 26–28 2008.

[11] G. R. Milne and M. J. Culnan. Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2002 U.S. web surveys. *The Information Society*, 18(5):345–359, October 2002.

[12] D. Reinhardt, J. Borchard, and J. Hurtienne. *Visual Interactive Privacy Policy: The Better Choice?* Association for Computing Machinery, New York, NY, USA, 2021.

[13] I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman. "won't somebody think of the children?" examining coppa compliance at scale. *Proceedings on Privacy Enhancing Technologies*, 2018(3):63–83, 2018.

[14] N. Samarin and P. Wijesekera. Understanding how third-party libraries in mobile apps affect responses to subject access requests.