May 2023

Pragmatic Privacy Innovation: SBOMS and Privacy Engineering and What’s Next

Michelle Finneran Dennedy
CEO, PrivacyCode.ai

Stuart Lee, PhD
VP &CPO, VMWare

Privacy+
Security
Forum

Speakers

Privacy+ Security Forum

Michelle Finneran Dennedy

CEO
PrivacyCode, Inc.

Stuart Lee, PhD.

VP & CPO
VMWare

What’s a BOM?

Bill of Materials

1920s - Ford Motor Company, which developed a detailed BOM for the production of the Model T automobile.

- The BOM listed all the parts and components required to build the car, along with their specifications and quantities.
- enabled greater standardization and efficiency in production processes.
- optimize its supply chain, reduce waste, and speed up production times.

Turney, M. C. (2015). Bills of Materials in Manufacturing: Definition, Types and Applications. Nova Science Publishers.

Single Bill of Materials (sBOM)

2018 – NIST introduced the sBOM in their 2018 publication, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks".

- IoT devices develop an sBOM to list all the software components and dependencies used in their products, to help identify and mitigate potential security vulnerabilities.
- Now used in other sectors such as automotive, healthcare, and aerospace, to ensure the safety and security of products.

https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks

To BOM or Not to BOM?

- In May 2021, the US government issued an executive order requiring federal agencies to include sBOM requirements in their contracts with software vendors, to improve the security and transparency of software supply chains. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Former Privacy Commissioner and Practitioner, Joanne McNabb has advocated for the PBoM. McNabb, Joanne. "A Privacy Bill of Materials Could Help Address IoT Security Risks." IAPP Privacy Advisor, International Association of Privacy Professionals, 23 April 2019, https://iapp.org/news/a/a-privacy-bill-of-materials-could-help-address-iot-security-risks/.
- AND of course, PrivacyCode.AI helps users create automated and auditable PBoMs… (I may be a teeny bit biased!) See. PrivacyCode.ai

.

<u>BUT</u>

- Difficulty in obtaining comprehensive sBOM:
  - In many cases, software products can contain numerous third-party components and dependencies, which can make it difficult to obtain a comprehensive and accurate sBOM.
  - Some components may be hidden or difficult to identify, which can make it challenging to fully understand the potential security and privacy risks associated with a particular product.
- Risk of false sense of security:
  - Simply having an sBOM does not guarantee that a product is secure or free from vulnerabilities.
  - While an sBOM can provide valuable information about the software components used in a product, it does not necessarily provide insight into how those components are being used, how they interact with each other, or how they may be vulnerable to attack.
- Limited focus on privacy:
  - While sBOMs can help identify potential security vulnerabilities, they may not necessarily provide the same level of visibility into privacy-related risks.
  - Privacy risks may be more difficult to identify and assess, as they often involve data collection and processing practices rather than specific software components.

Privacy Engineering is a Team Sport

- Applying the concepts of PBoMs and SBOMs in the wild
- Leveraging standard practices in Privacy Engineering for efficiency
- How to Turn a PBoM into a Business enabler
- What the heck does AI do to all this mess??

DISCUSSION & CONSPIRACY

Aren't you glad you're here in the room??

Questions & Contacts

Michelle Finneran Dennedy

CEO, PrivacyCode.ai

michelle@privacycode.ai

Twitter: @mdennedy
LinkedIN: /michelledennedy

Dr. Stuart Lee

VP & Chief Privacy Officer
Organization

Lstuart@vmware.com

LinkedIN: /stuartleephd