May 23rd:Security, Standards and GDPR

Date: 23 May 2018

Location: Level 39 in Canary Wharf in London.

Agenda

Report & Event Produced By OpenConsent

Workshop Summary

On May 23rd OpenConsent as liaison to Kantara Initiative, held a seminar and workshop focused on the intersection of security, standards and privacy, looking to highlight industry requirements and gaps. The Kantara Initiative, the British Security Industry Association, the Security Industry Association (USA), KrowdThink, Gluu and My Life Digital sponsored the workshop.

The workshop provided a networking opportunity across trade associations and jurisdictions to increase awareness of industry privacy efforts and guidance, in addition to discussing privacy guidance gaps and frictions in security system deployments, throughout the supply chain, from product provider, to system integrator, to end user.
The GDPR relies heavily on an understanding of industry best practices to interpret law into accepted guidance. This workshop lays foundations for the capture of security industry best practices.

In Attendance

The seminar audience included security system providers from both the digital and physical security spheres, providers of security system integration services, event management services, end-users and subject matter experts. In addition, we had significant participation from EEMA in the workshop as the Executive Director Jon Sharma led questions and comments.

The workshop identified, examined and discussed standards, codes of conduct and best practices for the deployment of security systems and solutions. It examined the extent to which these practices addressed more defined privacy requirements in the GDPR and across many of these cases the gaps that exist.

Presentation: Sal D’Agostino: Security & Privacy Standards

Presentation

As a set-up to the workshop a review of surveillance including ANPR and the use of video cameras in the UK was presented to the audience. This included a number of items that sets up the UK as having multiple components of what is best practice based on experience (world’s first commercial plate reading in the Dartford Tunnel in 1979), the fact that a surveillance commissioner exists and that a code of practice for surveillance exists covering general surveillance, license plate reading, body cameras and drones. A presentation from Kantara took the audience through the standards development process, and identified relevant privacy standards. The presentation also highlighted factors for successful adoption of standards including: the need to address security and privacy; ease of use (both from a human as well as a machine perspective when appropriate); interoperability across geographic, technical and use case scenarios; and stakeholder return on investment. The goal being to combine best practice with existing standards to develop specific guidance on privacy and security systems of immediate interest to those in attendance.

KANTARA INTRODUCTION Sal D” Agostino & Mark Lizar

Presentation

Introduced standards effort and the liaison with Kantara Consent & Information Sharing WG, Identity Relationship Management & User Managed Access WG. Discussed overlaps and best practice.

Panel: Robert Lapes, Geoff Revil, Mike Schwartz, Mark Lizar:

A panel of subject matter experts from Capgemini, OpenConsent, IDmachines, Krowdthink and Gluu guided discussions with the audience on particular GDPR challenges for security infrastructure for providing context specific privacy rights and notice for surveillance, highlighted in the workshop. The participants were keen to learn practical and tactical immediate steps they could take to be compliant with the GDPR.

Discussion

In many cases the members of the audience whether providers, integrators or end-users were most interested in concrete guidance. Literally, “tell me what to do and how to do it”. The subject matter experts gave specific examples based on their experience and knowledge of common security use cases with the audience members.

The topic of cyber physical considerations and the implications of mobile devices and physical security infrastructure being combined.   This puts into play multiple security contexts for data breach and privacy impact assessments including mobile device security as well as hardening network endpoints in particular IP surveillance cameras. References were given to hardening guides developed by the presenters for cameras and video management systems that were publicly available. A great deal of the security and surveillance contexts are dictated by the authority that is used to collect and process. The event use case was discussed as it was something where multiple participants have direct experience. In particular the challenges required to stand something up from literally the ground up with sometimes little pre-existing relationships between the multiple event stakeholders, organisers and event management.

Key Points:

Round table question and answers-

- Not every surveillance activity is balanced, but notice is required as best practice at some point for the user where the GDPR is applicable.
- Physical security is overt surveillance and as such the surveillance needs to be addressed directly.

- The supply chain needs to increase transparency over data security in particular the steps being taken to improve secure communications as well as encryption of data at rest and at motion. This is a practice that is seldom fully achieved in most video surveillance and physical security deployments.

Points for GDPR Guidance

- Evolving references and best practice in consent management and access control being taken into account are critical for surveillance systems.
- When and under what authority are privacy services to be made available for security? Better to be expansive in the services that are made available.
- Privacy information should be available for every security and surveillance deployment:
    - Primary information is the authority unto which the security and surveillance operates under.
    - All privacy legislation require a minimal set of information for security.
        - Providing privacy and security notices, addressing general inquiry, even in the case where privacy by design has been implemented, and/or where there is no surveillance, is best practice. This needs to include a digital and/or physical notice for security and privacy contact besides reference to policy.
    - Data retention policy best practice and guidance is needed from the data controller. There can be conflicts between data retention requirements for security purposes and data minimization. This is a critical component for an operational privacy policy.
        - Calculating data retention - a key topic for next event
- Security and surveillance is vulnerable-because it infringes privacy and is likely to draw scrutiny from regulators as well as privacy advocates.
- GDPR provides guidance to balance surveillance with transparency and trust frameworks.

Key Issues:

- How do you protect the security infrastructure from privacy attacks?
- For public systems, if there is no opt in, what is best and operational practice for opt-out (or to restrict processing) ?
    - What specifications and standards apply?
        - Surveillance commissioner code of conduct
        - ISO, BSI, NIST cybersecurity and privacy frameworks.
- Systems are vulnerable to privacy compliance risk from vendor to installer to end-user
    - Combination of processor and data controller in the surveillance operator without explicit enumeration, a priori, of data subject further complicates matters.
    - System logs have an important role to play.

- Ecosystem level
    - Opportunity for industry to take the lead
    - Trust platforms need to ensure transparency –surveillance industries too (not only other consent systems) - standard for transparency

Baseline Use Case (non-CCTV)

WiFi & Device Security and Privacy Risks

WiFi service providers think they operate with the authority of legitimate interest and that this is balanced in the public good?

- Mobile device, tracking by service and application providers, data leakage, and key personal data resources- i.e. contact info, privacy notice format for providers for transparency over data sharing as one key aspect in security reporting.
- Recent Facebook revelations about data sharing with mobile operators shows how the status quo is rife with privacy risk.
- Open Consent is putting in place a Signal Test that looks to examine the extent to which rights are usable and accessible.

Summary

Globalization and digitalisation of policy means standards are required to map to each other for privacy and security. Most standards development organisations are updating security guidance and controls to be more inclusive or privacy risk assessment, controls and best practice.

Many of the audience members were keen for follow up from the sponsors, SMEs and audience members and in most cases specific person to person (company to company) actions were established in the networking that rounded off the event.

Manufactures and implementers prefer;

- Privacy and security to be built in,
- İnteroperability and portability built in
- Usability-user experience built in

Follow Up

A next event for standards and interoperability is being organised for moving forward codes of practice in industry across trade associations and the security and safety ecosystem for new EU and international privacy requirements.

If you would like an invite to the next workshop July 19th, 201 8email events@openconsent.com. If you are interested in the next event report email security@openconsent.com

OPEN CONSENT

Outtakes

Kantara & OpenConsent leading outreach in security industry

kantara
INITIATIVE
Ethics & Conformance Trust Marked
Nurture. Develop. Operate.
– that's what we do
colin@kantarainitiative.org
Twitter:
@KantaraColin
@KantaraNews
Join us at https://kantarainitiative.org/membership/