Securing the Connected Future

Inside Telecom conference, Strømstad

Geir Bjørndal

May 2018

Expanding Global Profile

CUSTOMERS

924 CUSTOMERS

Powered by Verimatrix

SCREENS

200 MILLION DEVICES

Addressed and protected

COUNTRIES

113 COUNTRIES

Deployed and supported

Trusted by All Major Content Studios

Verimatrix is doing

- Conditional Access(CA)
- Digital Right Management(DRM)
- Watermarking
- IoT Security
- Secure Analytics

Challenges in collecting and storing data in a secure way

New challenges for Operators who wants to collect and store data in a secure way

- Cloud connectivity
  - Everybody connected to everything
  - Securing info increasingly important
- Multivendor Environment
  - Several vendors
  - Complex systems
  - More opportunities for leaks
- Hackers(Internal and External)

High profiled breaches

- Cox Communications
  - Customer databased hacked
  - 6 Mill customer accounts
  - Fined 595k US$ by FCC
- Target
  - Credit card info exposed
  - US$ 260 M in expenses to settle
- Vizio – analytics data snatched in a man in middle attack
- Facebook – not a regular hack, but more misuse

The New Complexity

- Hacking and exposing data
  - Operators are often held liable in the event of security breaches, and harm to the operator's public image is not exactly a competitive advantage — impacting relationships with suppliers and clients.

- Tracking viewership on unmanaged devices
  - Operators must ensure the protection of not only content and entitlements, but also the integrity and security of census-level data provided to partner stakeholders

- Security and integrity of viewing data
  - The ability to monetize video analytics data relies on data exclusivity, which is compromised in the event of a data pathway breach

General Data Protection Regulation

- Companies must obtain informed consent from all consumers to collect data, including verification that minors have the consent of their parent or custodian
- Consumers can withdraw consent and erase collected data at any time (i.e., the right to be forgotten)
- Companies cannot export data outside the EU to systems that do not meet GDPR standards

General Data Protection Regulation

- Companies must establish a Data Protection Officer (DPO) who reports on the company's security systems.

- Maximum fines for a breach are the greater of €20 million or 4% of annual worldwide revenue.

TV operators have to be “trusted”

- Preserving trust with their customers is a key competitive advantage for operators at a time of heightened competition
- Operators are scared to collect information due to the fact that they are viewed as trusted and will not risk this position
- I have met operators who do not want to collect too much user information as they are scared of internal misuse

Who Has the Keys? Developing Data Security Systems

Service operators are faced with three options when it comes to video analytics data security:

- Develop systems internally
- Outsource systems to third-party solutions providers
- Employ a mixed model approach that blends both internal and external solutions

Sort of conclusion

- Securing video analytics data must be a constant priority, not a periodic responsibility, to ensure the security and integrity of the data

- With an increased reliance on video analytics data for service-related decisions, ensuring the integrity of the data and trust of the customer has become a board-level responsibility

- Operators understand that security of video analytics data is not their core business and are instead leaning on partners with security-specific expertise

Thank you.

gbjorndal@Verimatrix.com