MORRISON
FOERSTER

PRIVACY + SECURITY FORUM

Privacy in a Connected World: Tracking, Telemetry, and IoT

Presented by:

Christine Lyon, Partner, Morrison & Foerster LLP

Matti Neustadt Storie, Director, Privacy and Data Security Evangelist, NetApp

Agenda

- Understanding when “machine data” may be personal data
- Breaking down machine data into common categories for closer analysis
  - Registration data
  - Usage and log data
  - Cookie or similar tracking data
  - Telemetry data—often the most uncharted area requiring greatest attention
- Deeper dive into telemetry data
  - What is telemetry data?
  - What are the privacy and cybersecurity risks?
  - What additional issues arise for B2B providers?
- Action items and key takeaways

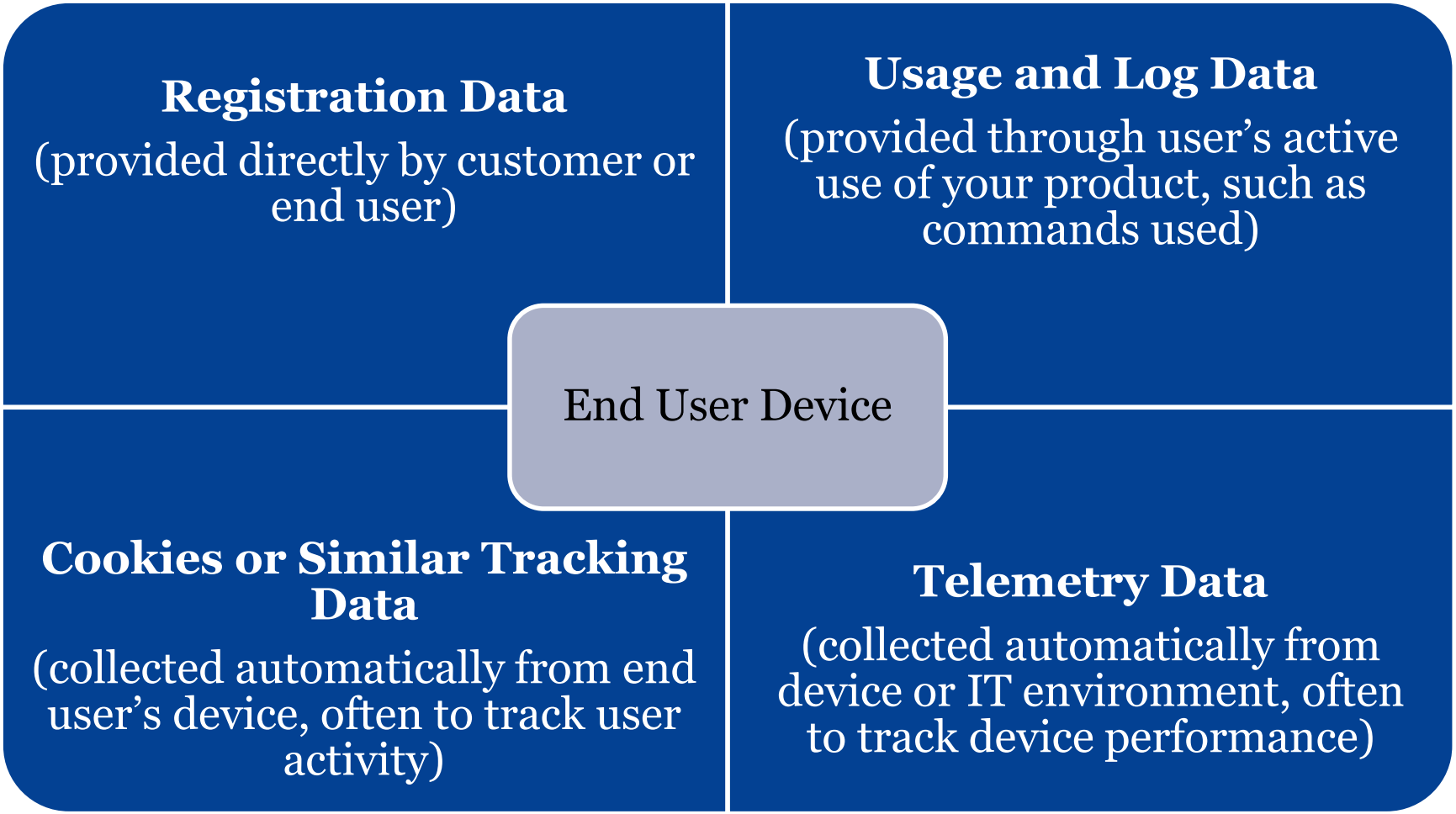
Machine Data, Personal Data, or Both?

Companies are collecting more and more "machine data" related to devices (e.g., telemetry data)

This data may be intended to monitor devices rather than people, but it's increasingly likely to be personal data too (e.g., CCPA, GDPR)

Companies will need to take a closer look at device data in their privacy governance programs

Basic Categories of Device Data



Registration Data

What Type(s) of Data?	When/Why Likely to be PI?
Data registering an end user's device with the provider of a service to the device: • Might be B2C customer activating device or application for personal use • Might be B2B customer activating devices or applications for business end users Potential uses: • Managing commercial relationship (billing, product notifications) • Monitoring security	Typically includes direct personal identifiers such as name, user name, email address, etc., as well as device identifiers In turn, any other data associated with the device may be linked to that PI as well

Usage and Log Data

What Type(s) of Data?	When/Why Likely to be PI?
Data about a user's activity on a device, such as activity records Potential uses: • Improving current products • Developing new products • Marketing and upselling	PI if associated with a user ID, user credentials (e.g., passwords, hashed password, token), or other individual identifiers • *Example*: Acme Company creates a user ID called "admin" for its designated IT administrator—sounds generic but still PI because relates to an individual • *Example*: identifier is a string of numbers that doesn't contain name, email address, other human-readable elements, but still allows our system to recognize that user

Cookies or Similar Tracking Data

What Type(s) of Data?	When/Why Might it be PI?
Data collected automatically from end user's device by cookies or similar mechanisms (e.g., pixel tags) • Cookies can be session cookies (session ID, date/time/activity) or persistent cookies (assigning a machine-readable identifier to a user's browser or device, to recognize the user/device across time and multiple interactions) • Includes first-party as well as third-party tracking • Even if a user declines non-essential cookies, essential cookies might still be placed • RIP for third-party cookies?	Typically PI if the device is used by an individual (like a user, storage administrator, or customer employee), even if you don't know who they are by name or have the ability to contact them directly If you can distinguish the device and recognize it over time, that signals that some type of PI is involved

Device Fingerprinting: Post-Cookie Tracking?

What Type(s) of Data?	When/Why Might it be PI?
Typically refers to collecting technical information about a device (e.g., screen resolution, language, OS, fonts installed) to identify that device over multiple interactions Tend to be used where cookies fall short, such as on mobile devices or where the user has disabled cookies--and is potentially much more intrusive	Same analysis as cookies: • Typically PI if the device is used by an individual (like a user, storage administrator, or customer employee), even if you don't know who they are by name or have the ability to contact them directly • If you can distinguish the device and recognize it over time, that signals that some type of PI is involved

Telemetry Data

What Type(s) of Data?	When/Why Might it be PI?
Typically machine data collected from an IT environment for diagnostics, services, and support, such as: • File names, file path names • Device names, host names, domain names, serial numbers No standard/uniform definition; "telemetry data" also might be used to include system activity more generally (e.g., usage data, logs, activity data)	May include direct identifiers of end users (e.g., name or user name), depending on what the company considers to be telemetry data May include unique device identifiers of end user devices May include information about user activity, such as user activity that triggers alerts reported in telemetry data File names or other configurations might contain or reveal PI

Potential Examples of Telemetry Data

- Device identifiers
- Physical environment data from IoT sensors
  - Temperature, moisture, movement
- Device performance data
  - Power levels, power consumption
  - Response times
- Event data
  - Crash reports, potential security alerts
- File names, file path names
- Device names, host names, domain names, serial numbers
- Geolocation data

No standard/uniform definition; “telemetry data” also might be used to include system activity more generally (e.g., usage data, logs, activity data)

Comparison of Telemetry with Cookies

Cookies and Similar Tracking Data	Telemetry Data
Collected automatically from device, usually via website or other online activity	Collected automatically from device or customer's IT environment, usually via installed software or sensors
May be used either B2B or B2C	Same
Tends to focus on understanding end user behavior	Tends to focus on understanding performance of technology—but also may capture end user behavior
In EU, ePrivacy implications on top of GDPR	Same—note that ePrivacy rules are not limited to cookies
Potential CCPA "sale" issues for third-party cookies	CCPA "sale" issues less likely to arise—unless sharing with 3rd parties?

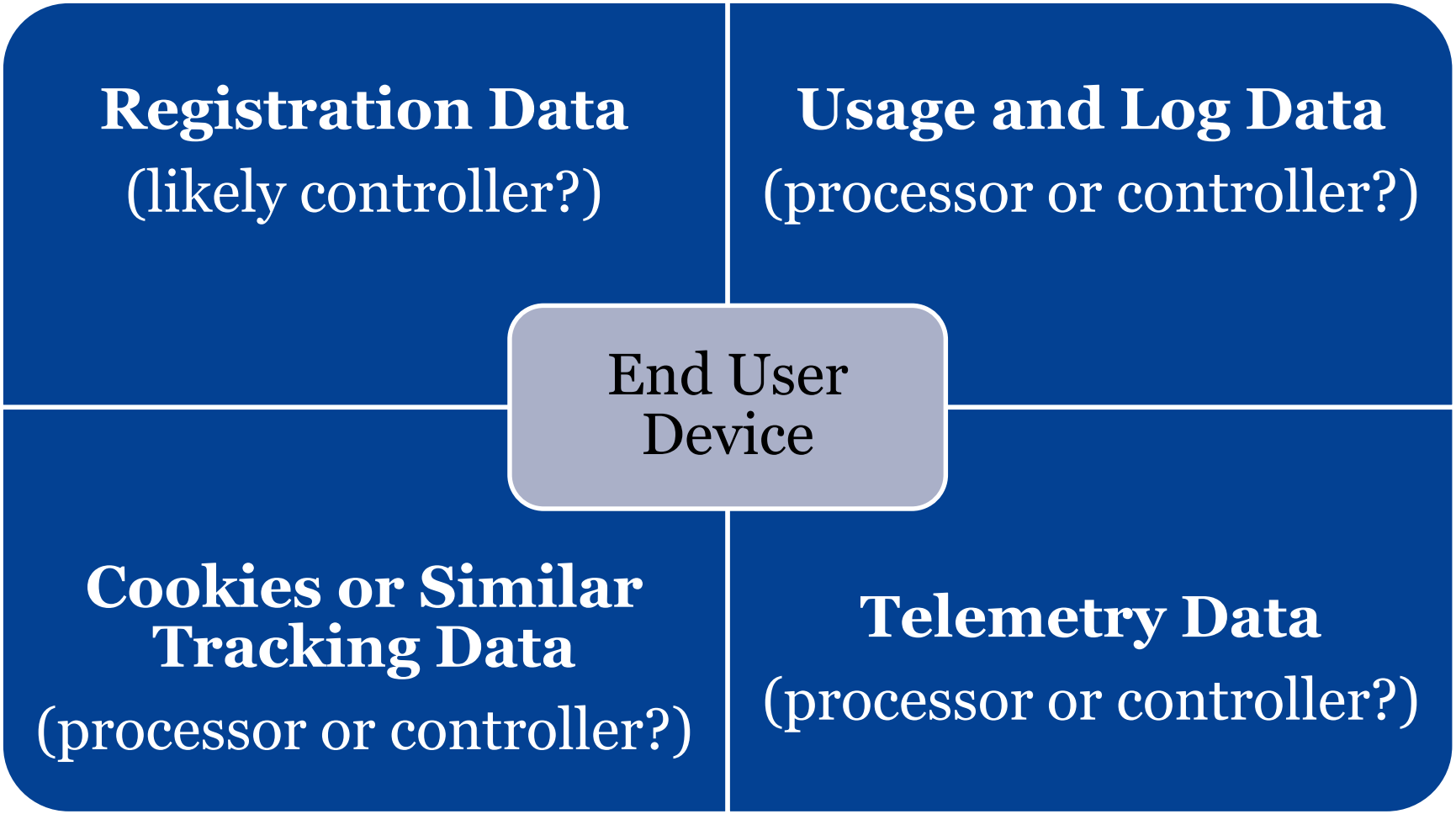
Risks of Failing to Address Telemetry Data

- Regulatory/enforcement actions
  - Example: Dutch DPA's lengthy scrutiny and DPIA of collection of telemetry data in Microsoft products
- Civil litigation
  - Example: class action lawsuits now spreading to UK and Europe as well, including against major U.S.-based B2B tech companies (e.g., see here)
- Breach of contract claims
  - Example: B2B provider promising to handle PI only as a processor, but using telemetry data as a controller
- Jeopardizing compliance certifications (like ISO 27001, NIST 800-171, or SOC 2) due to a failure to follow internal policies regarding PI

Additional Cybersecurity Considerations

- Security incidents exposing telemetry/device data
  - Covered by your security incident response plan?
- Misuse of data for spear-phishing, interception attacks, social engineering, spoofing, ransomware
  - User ID and configuration information can allow an attacker to impersonate a customer to gain unauthorized access to stored content through social engineering
  - Information like file directory paths and IP addresses can allow an attacker to "spoof" customer sites and interfere with a customer's business, or to set up "intercept" networks to eavesdrop on customer information flow
  - Telemetry data can allow an attacker to engage in "lateral movement" within the system to identify the highest value assets (like IP or sensitive PI) for ransoming, or to escalate privileges on key administrative networks to interfere with the effectiveness of backup, recovery, and business continuity plans
- Use of data for tracking or profiling end users or other individuals (e.g., users at customers)

B2B Providers: Controller or Processor?



Applying Privacy Principles to Machine Data

- Identify purposes for collection and processing
  - If B2B provider, determine whether handling that data as controller or processor
- Work with product team to apply data minimization principles
  - Identifying purpose(s) of collection
  - Collecting only the minimum data needed for those purposes
  - Retaining it only as long as needed for those purposes
- Assess where and how best to provide notice to customers, end users
- Evaluate whether necessary to seek consent or otherwise provide choice to customers, end users
- Expand Privacy by Design program to include relevant machine data

Key Takeaways

- ❑ Educate product teams and developers about machine data as personal data
  - ❑Ask clarifying questions and probe further if they say that they "don't have PII"
  - ❑Developing internal guidelines, training about the types of data that may be PI
- ❑ Address telemetry and other machine data as part of your internal privacy assessment process for products and services
- ❑ Leverage your existing privacy compliance program
  - ❑ Privacy by Design
  - ❑ Check existing notices, evaluate consents/choices provided
  - ❑ Manage data lifecycle consistent with data minimization
- ❑Ensure telemetry and other machine data are covered by your information security policies and security incident response plan


MORRISON
FOERSTER