You make **possible**

Privacy & Ethical Behavior for Innovation: AL, ML, and IoT

Tuesday, January 28 | 02:00 PM - 03:00 PM

Lisa Bobbitt, ARCHITECT.DATA PRIVACY,   @llbobbitt
Jelena Kljujic, TECHNICAL LEADER.SERVICES,   @Twitter_handle
Harvey Jang, VP. PRIVACY LEGAL   @Twitter_handle

PSO-2964

CISCO *Live!*

Barcelona | January 27-31, 2020

Cisco Webex Teams

Questions?
Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click "Join the Discussion"
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space
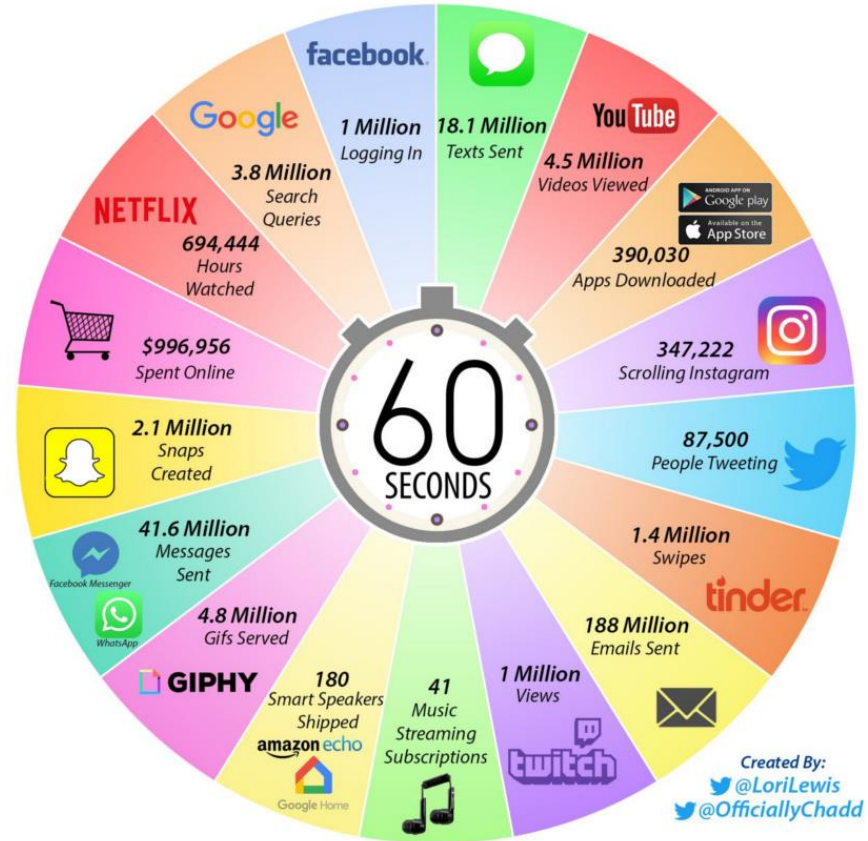

CISCO Live!

Agenda

- Introduction

- Data, AI, and Risk

- Human Rights, Privacy, & Security by Design & Default

- Ethical Analytics -> Privacy Engineering -> Secure Development & Operational Lifecycle

- Conclusion

Data Is Everywhere & Connecdted

- The vast majority of the **world's data** has been created in the last few years and this astonishing growth of **data** shows no sign of slowing down.

- The entire digital universe is expected to reach 44 zettabytes by 2020.

- In fact, IDC predicts the **world's data** will grow to 175 zettabytes in 2025. Let's dwell on that for a second: 175 zettabytes.

2019 This Is What Happens In An **Internet Minute**

- facebook — 1 Million Logging In
- Google — 3.8 Million Search Queries
- NETFLIX — 694,444 Hours Watched
- $996,956 Spent Online
- 2.1 Million Snaps Created
- 41.6 Million Messages Sent (Facebook Messenger)
- 4.8 Million Gifs Served (WhatsApp / GIPHY)
- 180 Smart Speakers Shipped (amazon echo / Google Home)
- 41 Music Streaming Subscriptions
- 18.1 Million Texts Sent
- YouTube — 4.5 Million Videos Viewed
- 390,030 Apps Downloaded
- 347,222 Scrolling Instagram
- 87,500 People Tweeting
- 1.4 Million Swipes (tinder)
- 188 Million Emails Sent
- 1 Million Views (twitch)

60 SECONDS

Created By:
@LoriLewis
@OfficiallyChadd

https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

cisco Live!

5

Gartner hype cycle

✓ Deep Neural Networks

✓ Conversational AI

✓ Virtual Assistants

✓ Knowledge Graphs

✓ Smart Workspace

Gartner Hype Cycle for Emerging Technologies, 2019

Expectations

Biochips
AI PaaS
Edge Analytics
5G
Autonomous Driving Level 5
Low-Earth-Orbit Satellite Systems
Edge AI
Graph Analytics
Explainable AI
Personification
Knowledge Graphs
Next-Generation Memory
Synthetic Data
3D Sensing Cameras
Light Cargo Delivery Drones
Transfer Learning
Emotion AI
Flying Autonomous Vehicles
Augmented Intelligence
Autonomous Driving Level 4
Nanoscale 3D Printing
Decentralized Autonomous Organization
DigitalOps
Adaptive ML
Generative Adversarial Networks
Decentralized Web
AR Cloud
Immersive Workspaces
Biotech - Cultured or Artificial Tissue

Innovation Trigger | Peak of Inflated Expectations | Trough of Disillusionment | Slope of Enlightenment | Plateau of Productivity

Time

Plateau will be reached:
○ less than 2 years   ● 2 to 5 years   ● 5 to 10 years   ○ more than 10 years   ● obsolete before plateau

As of August 2019

gartner.com/SmarterWithGartner

Source: Gartner
© 2019 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner®

CISCO Live!

Innovations Process Data From Multiple Sources to Make Decisions, Personalize Experiences, and Add Value to the Digital Experience

Continuous
Data

Decisions

Smart Cities, Smart
Cars, Smart Phones,
Smart Conference
Rooms

· Artificial Intelligence
· Machine Learning
· Deep Learning
· Supervised Learning
· Unsupervised Learning

CISCO *Live!*

Privacy, Fairness, and Ethics Controls Are Being Bolted On Given Customer Trust Issues
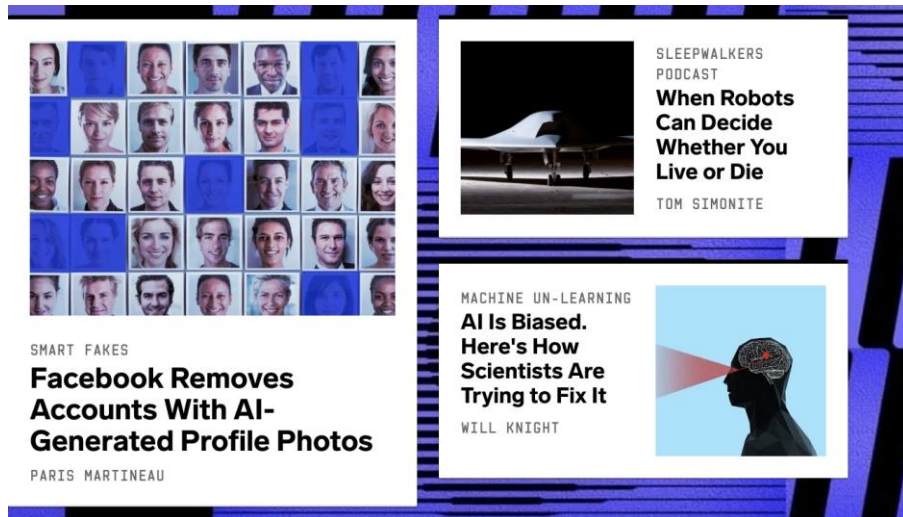
AI Risks
- **Autonomous weapons**
- **Social manipulation**
- **Invasion of privacy and social grading**
- **Misalignment between our goals and the machine's**
- **Discrimination**

Forbes

SLEEPWALKERS PODCAST
When Robots Can Decide Whether You Live or Die
TOM SIMONITE

SMART FAKES
Facebook Removes Accounts With AI-Generated Profile Photos
PARIS MARTINEAU

MACHINE UN-LEARNING
AI Is Biased. Here's How Scientists Are Trying to Fix It
WILL KNIGHT

CNN BUSINESS   Markets   **Tech**   Media   Success   Perspectives   Videos

FUTURE

The hottest product at CES 2020 is privacy

By Kaya Yurieff, CNN Business

PSO-2964   © 2020 Cisco and/or its affiliates. All rights reserved.   Cisco Public   8

Cisco AI/ML Trust Model

| Secure | Privacy & Fairness | Explainable | Transparent | Accountable |

TRUST
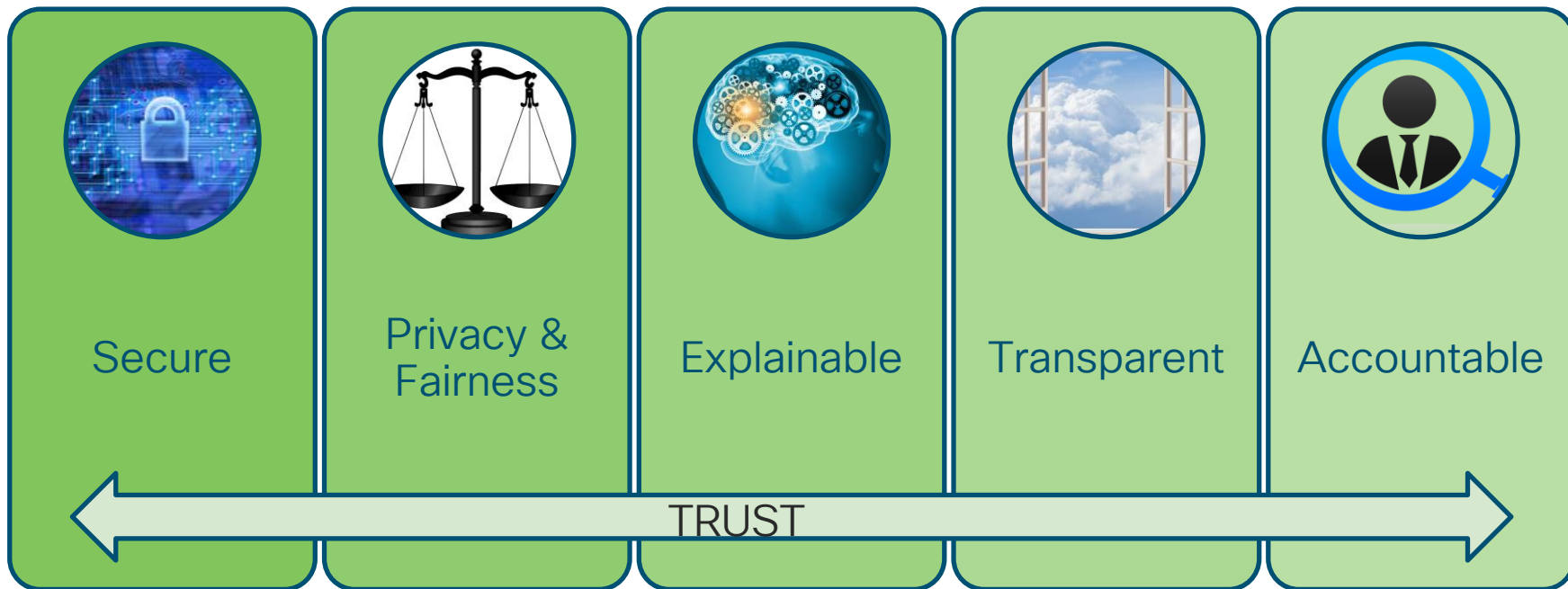
Threats, Vulnerabilities, and Risks

HR & Ethics
- Potential harm outweighs societal benefits
- Vulnerable groups may be underrepresented
- Data is biased
- Customers intentionally misuse the AI
- Unforeseen side effects
- Failure rates in use

Privacy
- Surveillance
- Interrogation
- Aggregation
- Identification
- Insecurity
- Secondary use
- Exclusion
- Intrusion
- Decisional interference

Security
- Data Poisoning
- Algorithm attacks
  - Reverse engineering
  - Code attacks
- Framework, Library mods
- Evasion techniques or coverage gap weaknesses
- Impersonation
- DoS
- DNS attacks

Human Rights by Design

- What is the responsibility of the platform company in these cases?

- Does societal bias constitute harm when reflected in AI?

- Can societal benefits outweigh individual harms?

- What is an acceptable failure rate?

- What if AI's failure rate is lower than the human rate?

- How do companies overcome limited leverage over customers, especially in the public sector?

- What is the appropriate level of care to ensure security?

Privacy by Design via Privacy Engineering

- Covers both the Product/Service Life Cycle and the Data Life Cycle

- Operationalizes Privacy by Design concepts

- Identifies the Data and classifies given value

- Driven by Your Privacy Policy

Product Ideation

P1: Value your data/Scoping

Plan

Develop

Monitor

P5: Continuous protection, management, and monitoring

P4: Be privacy transparent

P2: Know your data

P3: Protect your data: Assess & embed controls

Operate

Validate

Launch

Data Privacy Impact Assessment
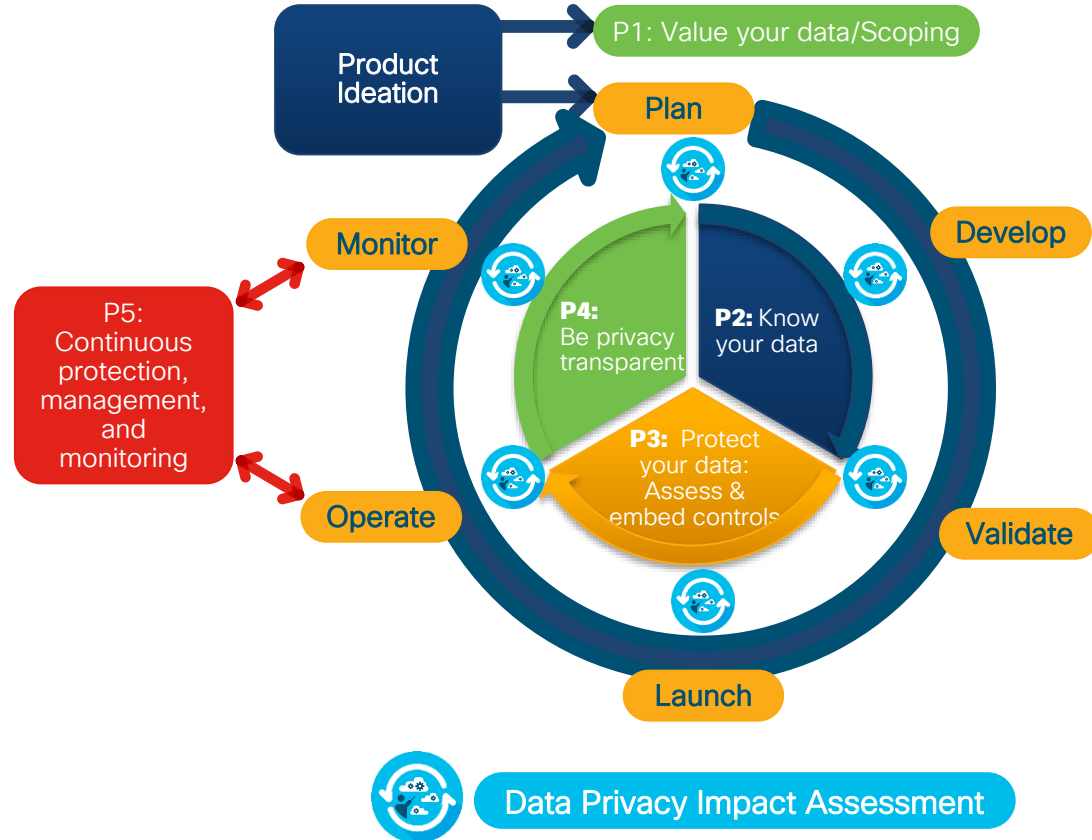
Embed privacy engineering into the secure development and operational lifecycle

- Establish privacy policy & requirements
- Data scoping workshop
- Threat Modeling

- Monitor changes in DPP policy/rqmts/control update with required remediation for Cisco, offers, and 3rd party processing

- Update privacy data sheet
- Update PIA & controls
- Operationalize
- Privacy controls

PLAN
Threat Modeling & Security Requirements

DEVELOP
Secure Modules & Static Analysis

MONITOR
Continuous Monitoring & Updates

VALIDATE
Security Vulnerability Testing

OPERATE
Security & Operational Management Process

LAUNCH
Security Readiness Criteria

CSDL
PHASE OVERVIEW
ConDev, Agile, Waterfall

- Privacy Impact Assessment (PIA); third-party contracts and assessments
- Embed privacy controls
- Update PIA

- Validate privacy controls
- Update PIA & controls
- Privacy data sheet, map data flows

Step 1: Privacy & Ethical scoping

Gather all your data and algorithms characteristics, security, privacy & data and Human Rights policies established by company culture, industry regulation or law

Work with your …

- Development
- IT
- Legal
- Industry compliance
- Records management
- Third-party providers

Know your policy

What market requirements, regulations, and corporate policies apply?

Whose data are you processing? Where did it come from? Do you have the legal basis to process it? Where is the data?

Where are your employees and customers?

What applications and algorithms are you running? What data do they process?

What data do you use in your processes

Whose data are you using? ? Is it created by your functions? Purchased from a 3rd party? Open Data Source?

Where is data stored? Is it secured? Which roles have access?

With whom do you share it? Will they provide the same level of the controls?

Where do you and your cloud providers securely process data?

What is your security plan for infrastructure, application, and product development?

Step 2: Assessment: Know your data
Inventory & classify your data & document its lifecycle

- Determine what **data is necessary** for your application/product

- Inventory your **data and its characteristics, confidentiality, fairness and privacy criteria** from your data policies (governance, protection, privacy)

- **Identify possible bias given the data demographics.**

- Identify and **tag your data context**

- **Outline your data lifecycle** as the data controller and/or processor
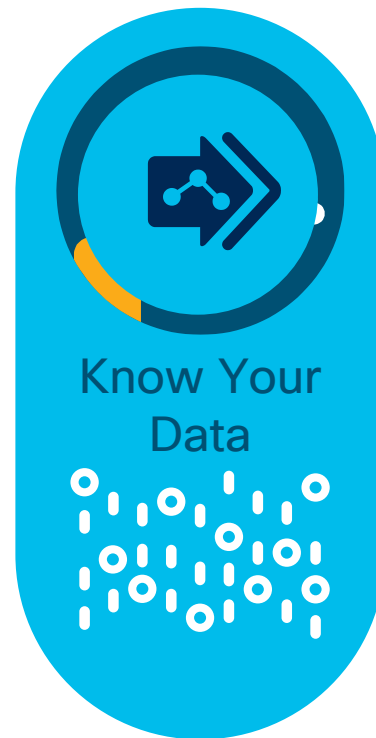
Know Your Data

Step 2b: Assessment: Know your algorithm(s)

Inventory & classify your algorithms & document its potential biases

- Determine what data is necessary for your algorithm.
  - Determine the bias of the data available given its demographics (recency, demographics, where, who, how long, etc)

- Determine Risk of Algorithm for Fairness
  - Risk that potential harm outweighs societal benefits
  - Risk that customers intentionally misuse the AI
  - Risk of unforeseen side effects
  - Risk that vulnerable groups may be underrepresented

Know Your Algorithm

Step 3: Set controls

- Establish your algorithms & data controls criteria per your data policies (governance, protection, privacy, ethics)
  - Example: legal basis in contract vs. opt-in consent
  - Example: Supervisored decisions given personal decisions

- Prioritize control requirements for data and context including third-party sharing, location, and legal basis under which you are processing
  - Example: financial data is restricted before announcement but is public afterwards

Legal basis
Data context
Transparency
Security
Collection limitations
Proportionality
Use limitation

Accountability &
operations requirements
Data minimization
Onward transfer
Retention & deletion
Individual rights
Fairness/ Bias

Step 6: Any change, go back to Step 1

Product Ideation

P1: Scope your data, algorithms, threats

Plan

Monitor

Develop

P5: Continuous protection, management, and monitoring

P4: Be privacy transparent

P2: Know your data

P3: Assess data & embed controls

Operate

Validate

Data Privacy Impact Assessment

Launch
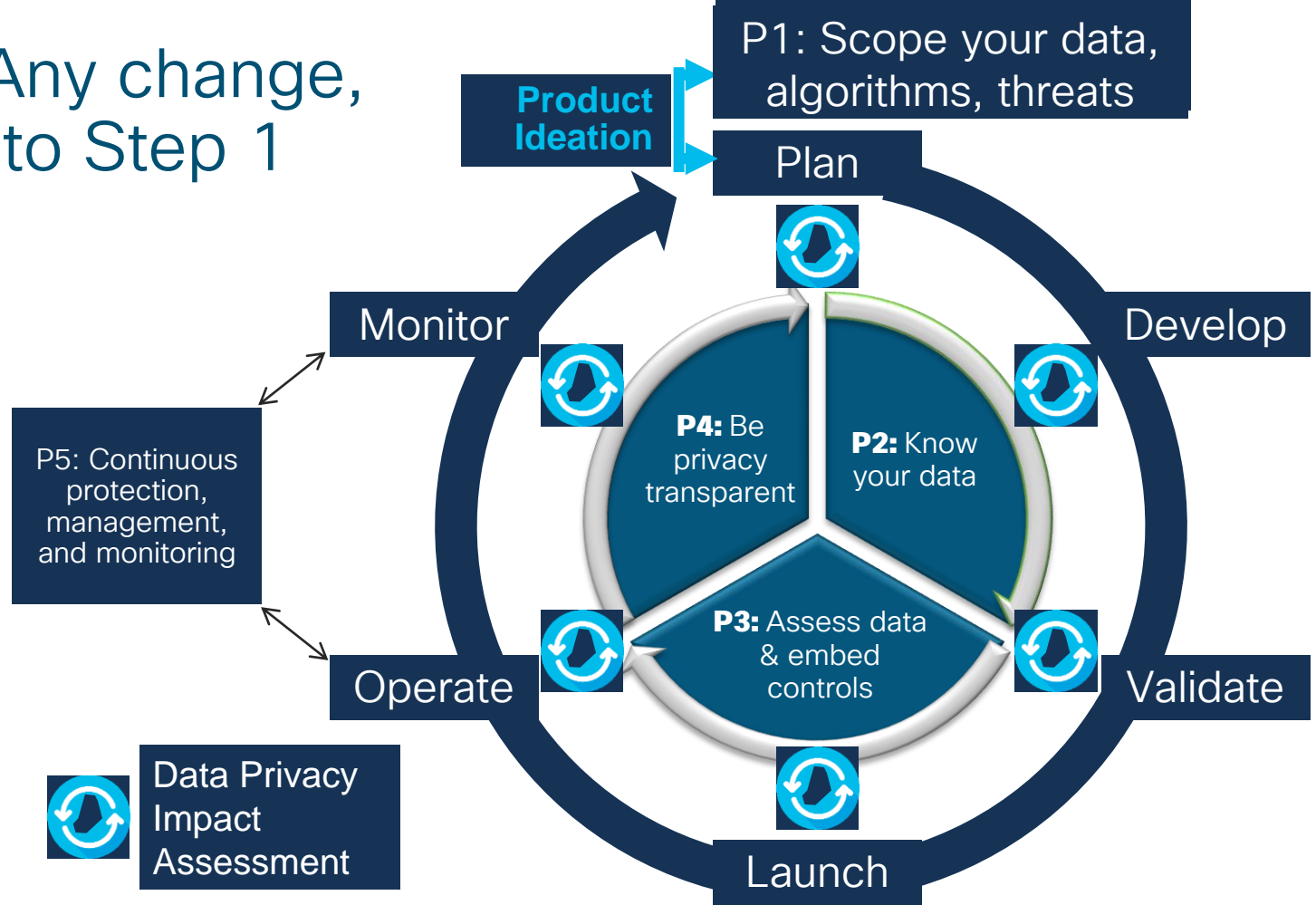
Step 3 (cont): Set controls

- Capture agile ethics and privacy-aware user stories

    As a business owner, I need to be able update end- and operation users' PII

    As a business owner, I need to know if any automated decision threatens a fundamental right of the users

    As an end-user, I need to be able to find the privacy notice within 1 click

    As an operations user, I need a mechanism to delete end- and operation users' PII on behalf of other end- and operation user

- Embed consistent ethicis and privacy-enhancing processes and technologies wherever possible

User needs

Process & technology

Step 4: Be transparent
Ethics, Privacy data sheets & data maps

Step 5: Operate & Monitor Controls

- **Establish a monitoring cadence** for all your processes including updating your PIA, checking on third-party processing, and measuring your response to requests re individual rights

- **Verify your technology controls** across solutions such as encryption at rest and in transit, identity and role-based access, and retention periods. Establish exceptions and automate where you can to monitor this

Digitize Where Possible

Why this Data Curation Framework: Its all about the data and how you process it ☺

- Digitization is taking advantage of the large volumes of data being produced, consumed, and stored locally, globally, and at the enterprise level

- This data and its context can be used for deriving business insights

- Curating helps connect business functions through common practices to efficiently deliver digitization and democratize data across the ecosystem

Curating Data

1. Assign your Data Steward(s)

2. Inventory your Data with its Classification and Purpose

3. Establish, Apply, and Verify Governance & Protection Controls
   - Remember these controls come from the customer agreement/contract &/or Cisco policy

4. Normalize Data for Interoperability
   - Type of storage, how it is updated, Legal Basis on which we collect/process

5. Reduce risk of PII and confidential data by
   - Summarizing, De-Identifying, Tokenizing, Anonymizing

6. Catalogue and Advertise Data, Data Characteristics and Controls

7. Manage the Sharing to Teams per purpose/contract specifics and their ability to provide the level of controls required by policy
   - Data Stewards are the source of truth for any negotiations on data

8. Maintain and enforce renewal, retention, and deletion schedules

CISCO Live!

Innovation Office: Privacy Engineering Innovate Everywhere

Global CX Centers: the on-ramp to Cisco

3,563 Active professional service projects

2.1M Cases handled annually

85% CXSAT

85% Of issues solved online every month

11,000+
Engineers
(blue + red badge)

1,525
Engineers have
1,804 CCIEs

860,000+
Parts delivered yearly
via **1,300+** depots in
138 countries

Digitized IC market trials

95%
Of product families
are creating IC

34%
Case avoidance for
all issues

95%
Of critical or warning
issues resolved by
customers

Global CX Innovation Office –Innovation Priorities

Case Deflection

Help the customer to become more self sufficient

Automate engagements for easy questions

Become proactive in alerting customers about risks before they become issues

Delivery Efficiency

Automate simple tasks and let our people focus on more complex ones

Use our knowledge to drive better quality and consistency

Direct Customer Value

What can we do to reduce effort for our customers across the lifecycle?

CX Innovation Organizational Context

Lightweight Software Development Methodology

CSDL flavor for Prototyping

Subject Matter Expertise

Example: Cisco Quick Answer Project

Cisco Customers

Cisco Internal Clients

SR#

SR URL

BDB

CSOne API

CSOne

Fronted/API

DBAS

Cisco IT LAE

User Generated Information
(incl case title, problem description, SR#)

User-to-Webex Teams

User Generated Information
(incl case title, problem description, SR#),
Webex Teams API, SR URL

Bot-to-Webex Teams

Cisco Webex

Teams
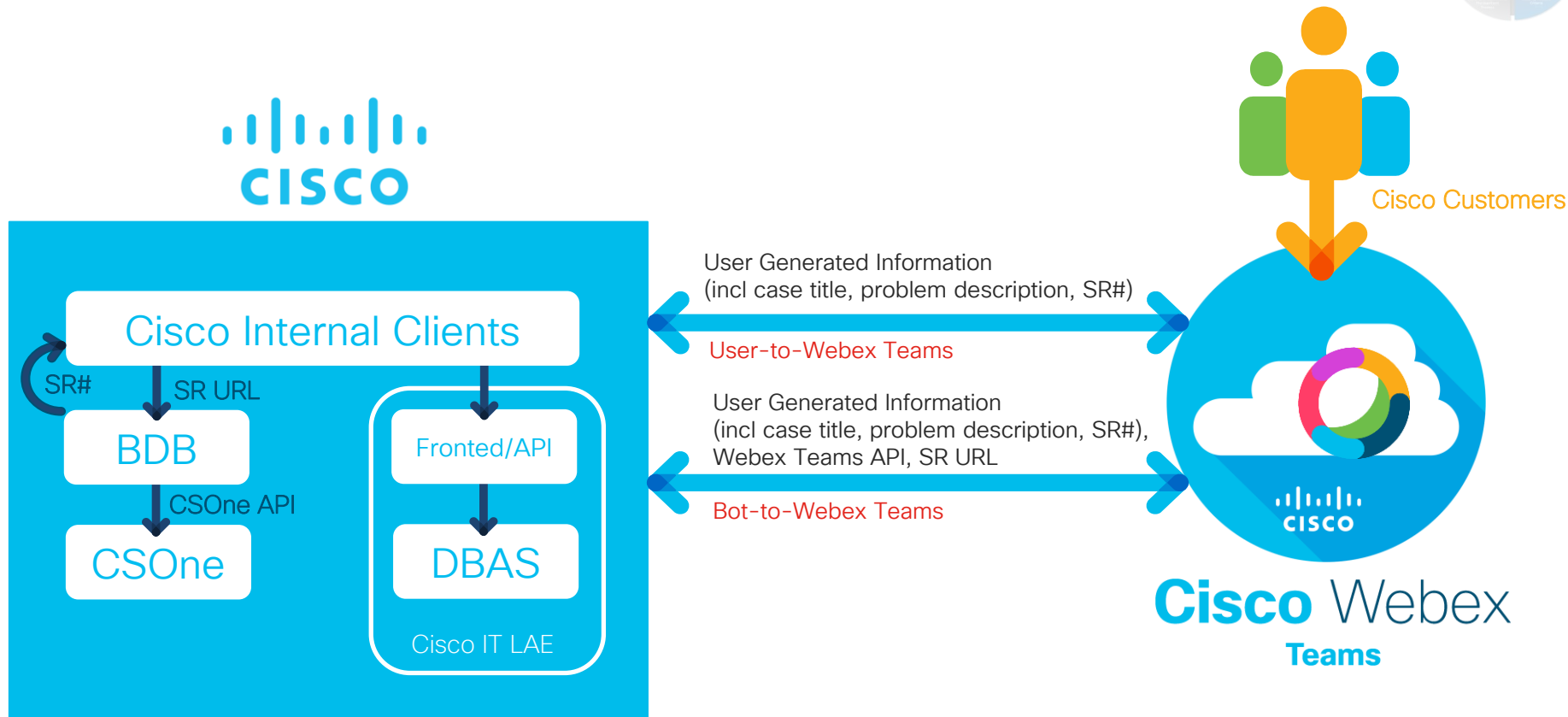
Spotlight: Candela

Ideate	Incubate

Idea originated and early development started within their work group
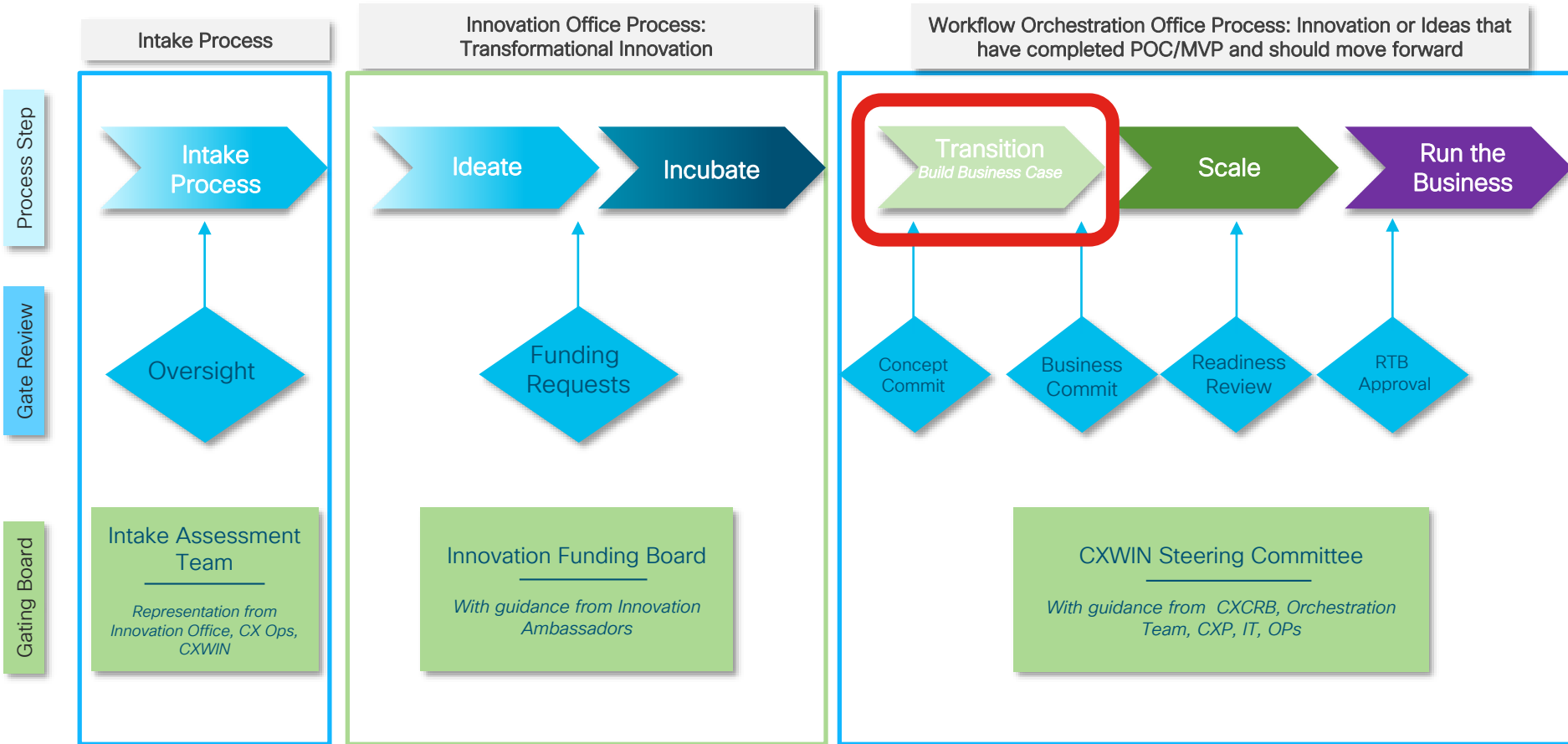
Solution to address three key challenges:
- Data Security
- Large Files
- Collaboration

Candela:
- Eliminates the need to download customer files for local analysis
- Makes files available from a single click within the engineer's workflow
- Enables collaboration by multiple engineers using the same version of the file

High Level End to End Process with Gates

Intake Process

Innovation Office Process: Transformational Innovation

Workflow Orchestration Office Process: Innovation or Ideas that have completed POC/MVP and should move forward

Intake Process

Ideate

Incubate

Transition
Build Business Case

Scale

Run the Business

Oversight

Funding Requests

Concept Commit

Business Commit

Readiness Review

RTB Approval

Intake Assessment Team

Representation from Innovation Office, CX Ops, CXWIN

Innovation Funding Board

With guidance from Innovation Ambassadors

CXWIN Steering Committee

With guidance from CXCRB, Orchestration Team, CXP, IT, OPs

Privacy Engineering in Innovation Office

On-demand training

Lightweight CSDL

Privacy Ambassador Network

Critical Privacy PSBs for Innovation Office-Lightweight CSDL

POLICY

- **SEC-DAT-KNOWWHAT**
  Know what data your offering or application is processing and document the required controls
- **SEC-PRV-DSRIGHTS** Rights of Personally Identifiable Information's Data Subject

DESIGN

- **SEC-DAT-MINIMIZE** Minimize collection of personal information
- **SEC-PRV-ERASE** Delete unneeded personal information

OPERATE

- **SEC-PRV-USERAUTH** Control user access to personal information
- **SEC-PRV-MANAGE** Allow users to manage personal information

"*Privacy is a fundamental human right, and we need security and transparency to protect it.*"

Chuck Robbins
Chairman and CEO, Cisco
February 7, 2019

cisco *Live!*

Sessions With a Privacy & Ethnics Focus Here at CiscoLive

- Privacy as a Business Enabler = PSO-2962

- Engineering Privacy By Design: A Webex Case Study on Privacy & Facial recognition & Other Personalized Innovations - PSO-2966

- Privacy and Ethical behavior for Innovation: AI, ML, and IoT - PSO-2964

- Cisco Webex and GDPR – BRKCOL-1797

- Cognitive Collaboration AI And Machine Learning Assisted Collaboration – BRKCOL-1460

- What will 2020 bring in application and network threats? - PAR-2995

- Webex Teams Security in depth = Part Two - Compliance, Policies and Data Loss Prevention – BRKCOL-279

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.

- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**