AI Security and Privacy Governance

Cebu, Philippines

December 2019

Alan Tang, PhD

FIP, CIPP/E/US, CIPM, CIPT, CISSP, CISA, PMP

HUAWEI

Huawei: Leading Global Provider of ICT Infrastructure and Smart Devices

Bring digital to every person, home and organization for a fully connected, intelligent world

Huawei's end-to-end portfolio of products, solutions and services are both competitive and secure. Through open collaboration with ecosystem partners, we create lasting value for our customers, working to empower people, enrich home life, and inspire innovation in organizations of all shapes and sizes.

At Huawei, innovation focuses on customer needs. We invest heavily in basic research, concentrating on technological breakthroughs that drive the world forward.

194,000

Employees

80,000+

R&D employees

170+

Countries and regions

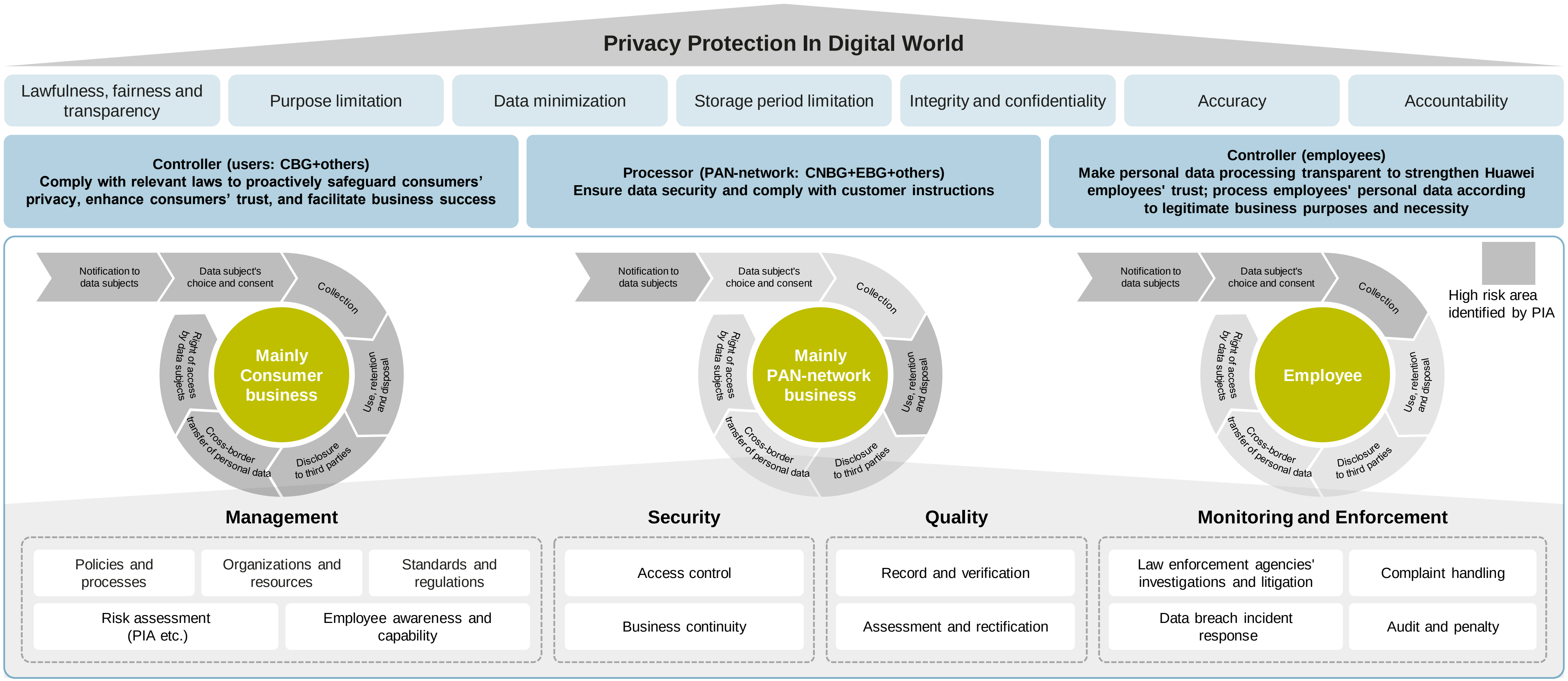
36

Joint Innovation Centers

61 in

Fortune Global 500

Set Differentiated Privacy Protection Objectives to Meet Various Privacy Expectations



Privacy Protection In Digital World

Lawfulness, fairness and transparency	Purpose limitation	Data minimization	Storage period limitation	Integrity and confidentiality	Accuracy	Accountability

Controller (users: CBG+others)
Comply with relevant laws to proactively safeguard consumers' privacy, enhance consumers' trust, and facilitate business success

Processor (PAN-network: CNBG+EBG+others)
Ensure data security and comply with customer instructions

Controller (employees)
Make personal data processing transparent to strengthen Huawei employees' trust; process employees' personal data according to legitimate business purposes and necessity

Notification to data subjects
Data subject's choice and consent
Collection
Use, retention and disposal
Disclosure to third parties
Cross-border transfer of personal data
Right of access by data subjects
Mainly Consumer business
Notification to data subjects
Data subject's choice and consent
Collection
Use, retention and disposal
Disclosure to third parties
Cross-border transfer of personal data
Right of access by data subjects
Mainly PAN-network business
Notification to data subjects
Data subject's choice and consent
Collection
Use, retention and disposal
Disclosure to third parties
Cross-border transfer of personal data
Right of access by data subjects
Employee

▨ High risk area identified by PIA

Management

- Policies and processes
- Organizations and resources
- Standards and regulations
- Risk assessment (PIA etc.)
- Employee awareness and capability

Security

- Access control
- Business continuity

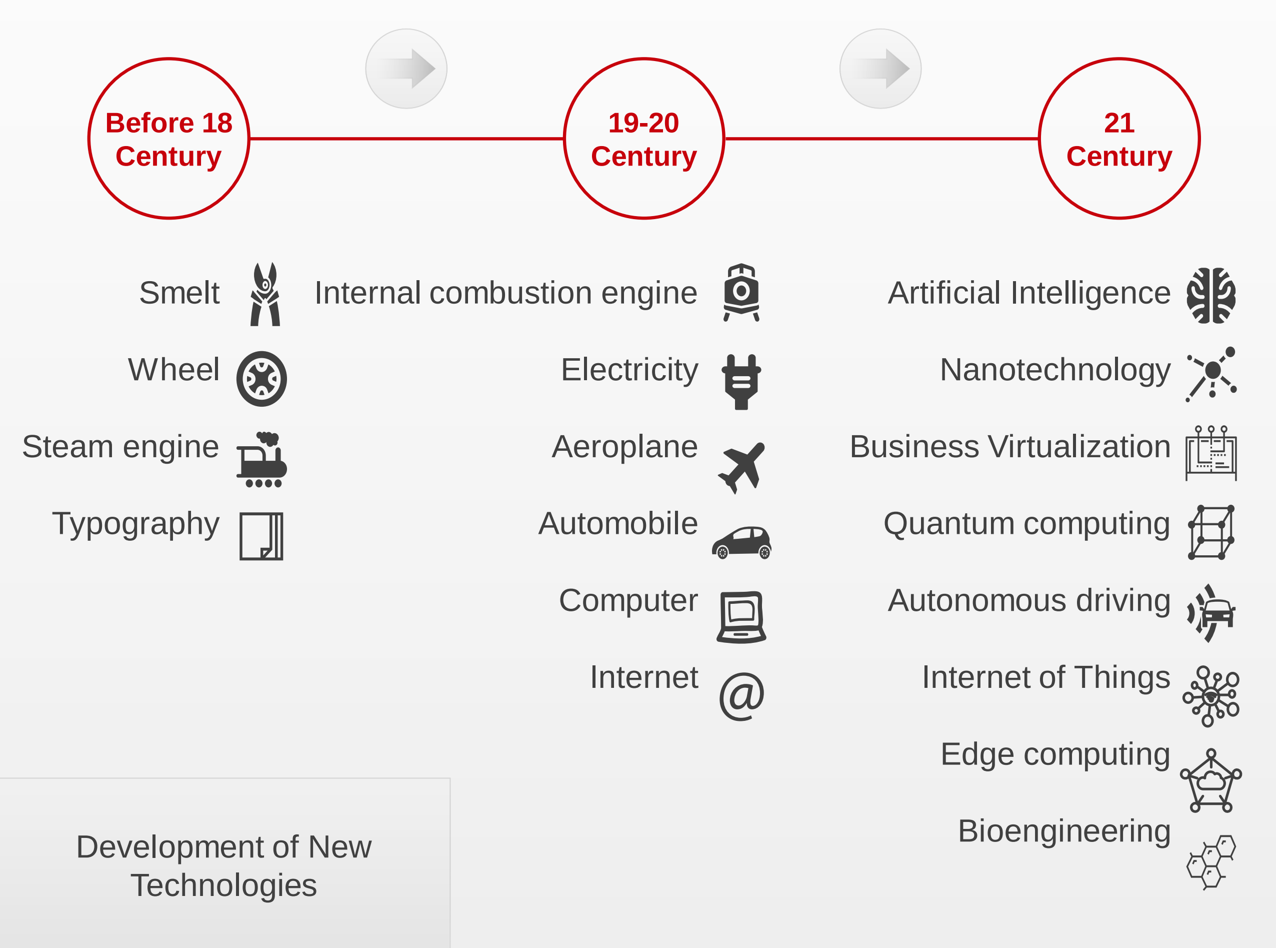
Quality

- Record and verification
- Assessment and rectification

Monitoring and Enforcement

- Law enforcement agencies' investigations and litigation
- Complaint handling
- Data breach incident response
- Audit and penalty

Technology Is Being Developed and Adopted Much Faster Than Ever Before



Before 18 Century

19-20 Century

21 Century

Smelt

Wheel

Steam engine

Typography

Internal combustion engine

Electricity

Aeroplane

Automobile

Computer

Internet

Artificial Intelligence

Nanotechnology

Business Virtualization

Quantum computing

Autonomous driving

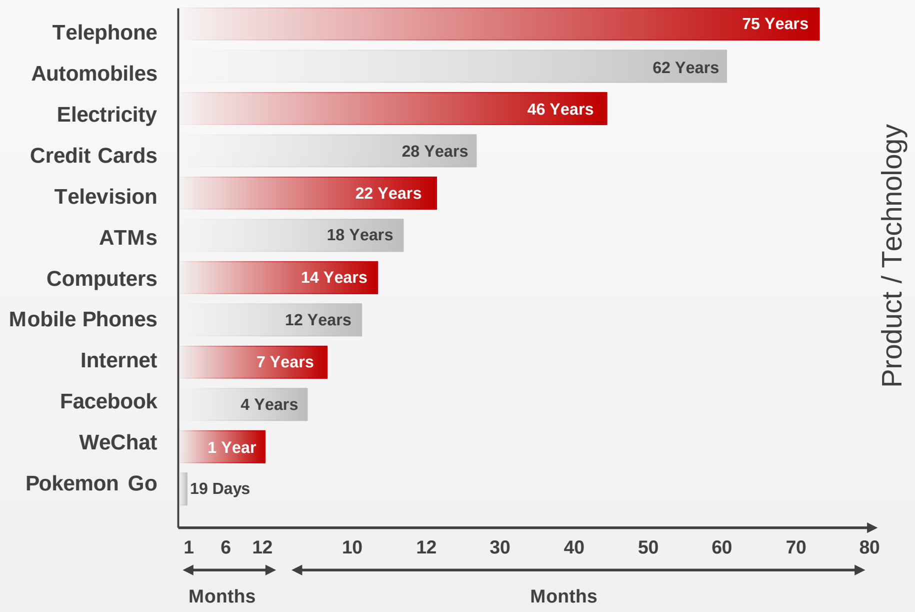
Internet of Things

Edge computing

Bioengineering

Development of New Technologies

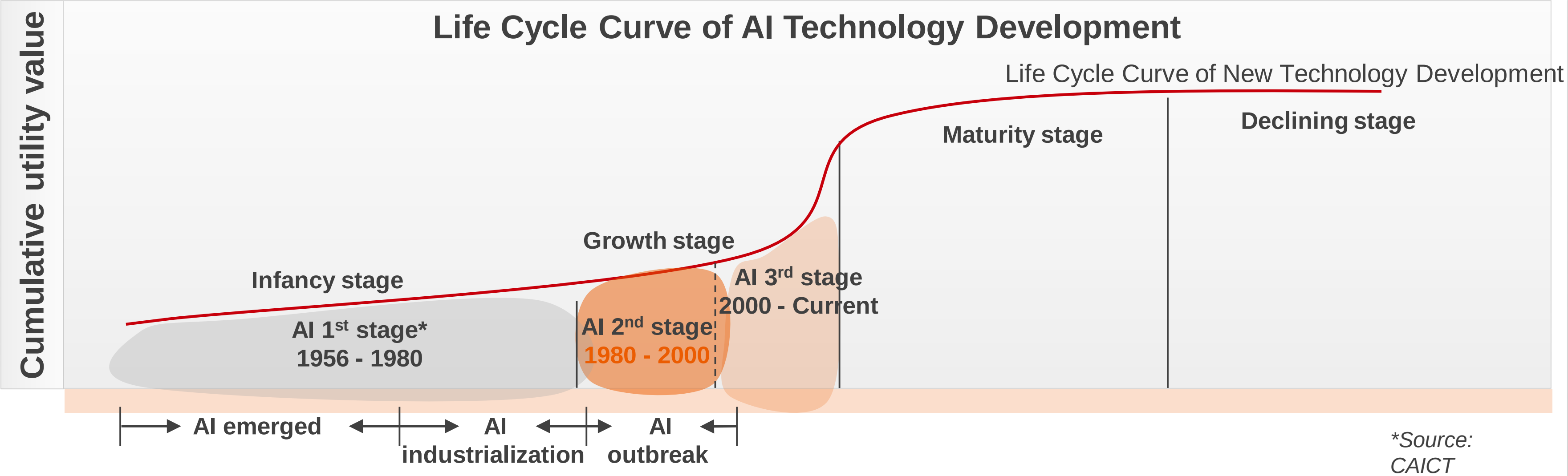
TIME TO REACH 50 MILLION USERS



https://blogs.wsj.com/economics/2015/03/13/it-took-the-telephone-75-years-to-do-what-dngry-birds-did-in-35-days-but-what-does-that-mean/

http://www.visualcapitalist.com/how-long-does-it-take-to-hit-50-million-users/

Technologies Are Rapidly Outpacing Policy and Legal Frameworks Especially in AI



*Source: CAICT

Laws and standards

AI stepping into growth step

- ✓ Many countries launched AI development strategy as fundamental national strategy
- ✓ Drafted AI ethical standards have been introduced.

- ✓ European countries, US and China have issued AI ethic and security standards and guidelines. And drafted industrial laws, for example, autonomous driving, have been continuously introduced.
- ✓ Organizations and ICT companies have introduced ethical and other AI governance principles and standards.

AI security and privacy governance stepping into practice stage

~ 2016 | 2017 | 2018 | 2019~

- Early adopters of new technologies can often seize the opportunity of transformation and become the industry leader.
- The regulations and laws of emerging technologies are often lagging.

Multiple Frameworks Are Being Formed Often Overlapping, Using Different definitions and Approaches. AI Will Compound The Issue

Influential Guidelines and Frameworks

European Union (EU)

- Ethics Guidelines for Trustworthy AI

The United Kingdom

- AI Auditing Framework

Singapore

- Model AI Governance Framework

IEEE

- Ethically Aligned Design (Version 1 - For Public Discussion)
- Ethically Aligned Design (Version 2 - For Public Discussion)
- Ethically Aligned Design (First Edition)

Harvard University

- A Layered Model for AI Governance

……

We have researched around 200 regulations, standards, principles, guidelines, study reports, whitepapers, etc.

- **Principles: humanity, , collaboration, share, fairness, transparency, privacy, security, safety, accountability**
- **Singapore Model Framework:**

Internal Governance Structures & Measures

Risk Management in AI Decision-making

Operations Management

Customer Relationship Management

AI Solution Provider

Organisation

Individuals

AI Applications Are Maximizing Available Technology. Cloud, Big Data, Global Connectivity

AI Use Cases

……

Challenges

Technical reliability

- DNNs lacking robustness may be susceptible to evasion attacks
- Complex systems such as DNNs lack transparency and explainability
- Data breaches, tampering, theft, and misuse

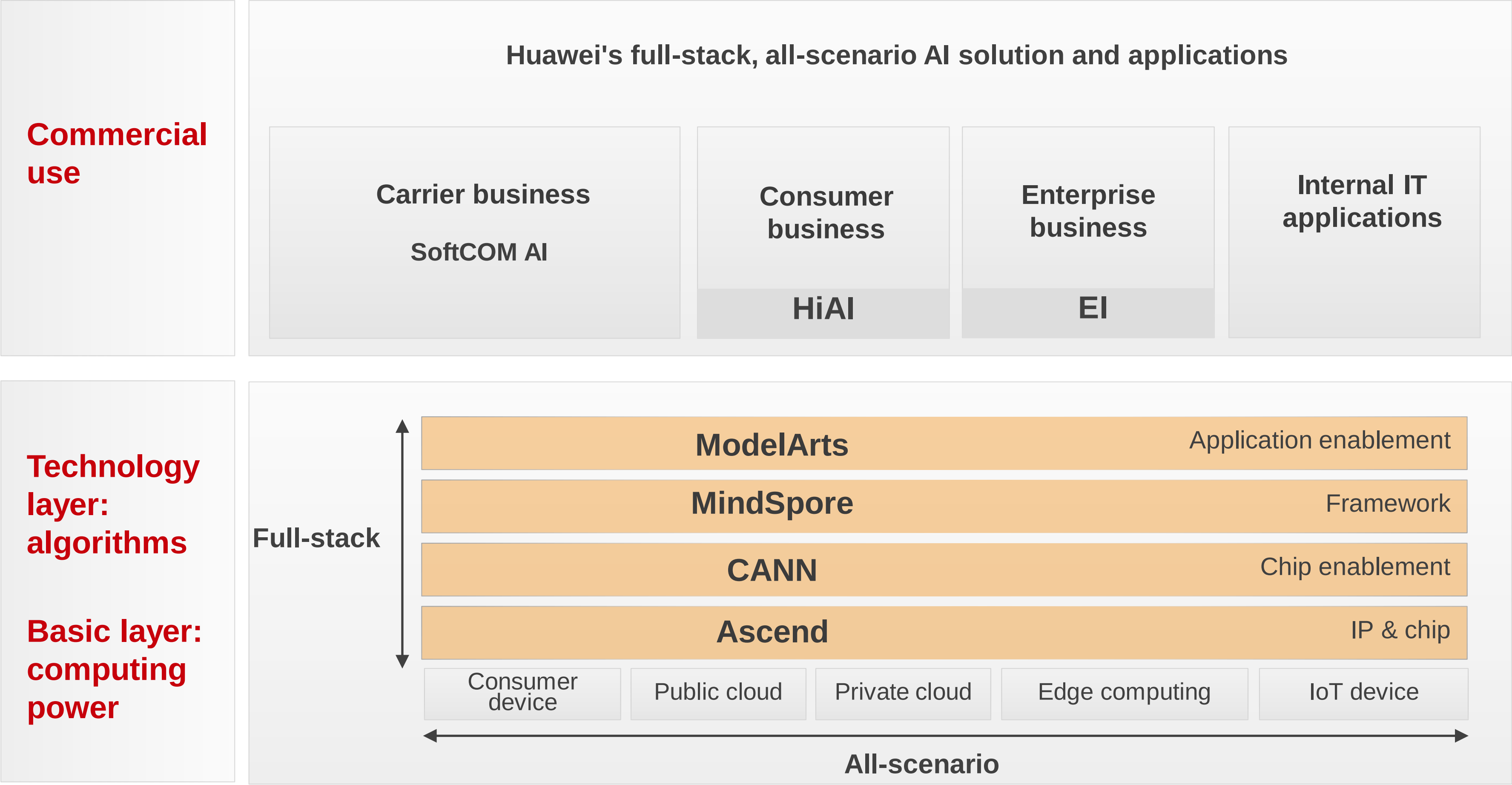
Societal applications

- The lack of control over the purposes may lead to AI being misused.
- Data quality issues may lead to biased and unfair judgments.
- Incompetent application developers and may misuse AI systems or cause security and privacy incidents.

Legal requirements and responsibilities

- No laws or regulations, such as regulations on autonomous driving and algorithm accountability, are available to clearly define the rights and responsibilities of stakeholders

What We Do Regarding AI at Huawei?



Commercial use

Huawei's full-stack, all-scenario AI solution and applications

Carrier business

SoftCOM AI

Consumer business

HiAI

Enterprise business

EI

Internal IT applications

Technology layer: algorithms

Basic layer: computing power

Full-stack

ModelArts Application enablement

MindSpore Framework

CANN Chip enablement

Ascend IP & chip

Consumer device | Public cloud | Private cloud | Edge computing | IoT device

All-scenario

SoftCOM

- RCA time shortened by 80%
- Power consumption reduced by 10% to 20%

HiAI

- Image recognition capability doubled
- 4500 images recognized per minute

EI

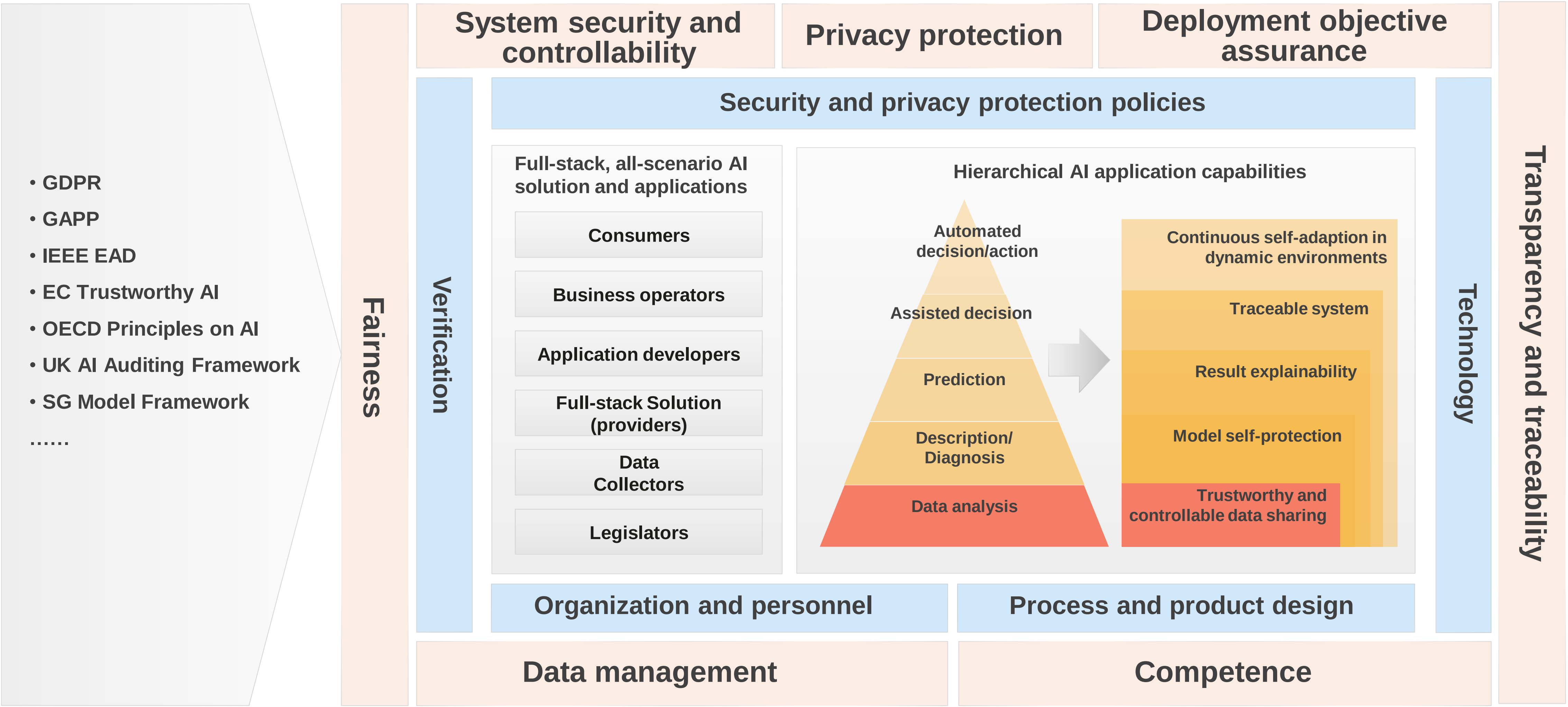
- Applied in 10+ industries
- 200+ specific projects

Huawei security products

- Advanced threat detection accuracy > 99%
- Secure O&M OPEX reduced by 80%

Secure and Reliable Full-Stack AI Assurance

Security and Privacy Protection of Huawei Full-Stack Solution and Applications



- GDPR
- GAPP
- IEEE EAD
- EC Trustworthy AI
- OECD Principles on AI
- UK AI Auditing Framework
- SG Model Framework

……

Fairness

System security and controllability

Privacy protection

Deployment objective assurance

Transparency and traceability

Verification

Security and privacy protection policies

Technology

Full-stack, all-scenario AI solution and applications

- Consumers
- Business operators
- Application developers
- Full-stack Solution (providers)
- Data Collectors
- Legislators

Hierarchical AI application capabilities

Organization and personnel

Process and product design

Data management

Competence

To Maximise The Opportunity Of ICT We Must Establish Partnerships for Trust and Confidence

- AI governance needs cooperation among various stakeholders, which expects AI stakeholders to review their work from the perspective of responsibility and provide a systematic approach to thinking and governance.
- Asia Pacific region is one of the tech innovation hubs in the digital world. We could take a lead.
- Asia Pacific region is committed to international and regional cooperation, and advocates a reliable and secure cyberspace.

In Summary

1. **Technology has always outstripped laws and regulations.**

2. **The cumulative impact of ICT, the global nature of supply chains and services amplify the legal gaps**

3. **Asia Pacific region as a global, stable, balanced region can take the lead in leading the debate and the solutions**

4. **AI utilises all ICT knowledge and capability – it will have profound implications – some we cannot see**

We should not wait for the challenges of ICT and AI to force a policy or legal framework, we should act now to create more practical policy and legal framework that maximise opportunity whilst protecting against unintended consequences

AI White Paper:
Thinking Ahead About AI Security and Privacy Protection

You can download here

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.