RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MLAI-T08

AI: Hacking Without Humans
How Can Human Brains Be Hacked?

Anthony J. Ferrante

Global Head of Cybersecurity and
Senior Managing Director
FTI Consulting
@FTICyber

Once a Fantasy – Now a Reality

We've come a long way since ***2001: A Space Odyssey (1968)*** and ***War Games (1983)***.

Today, the groundbreaking "super computers" of the silver screen are being realized through pocket-sized AI technology in Apple's ***Apple Watch***, Amazon's ***Alexa***, and Google's ***Google Assistant.***

Blurring the Lines Between Science and Science Fiction

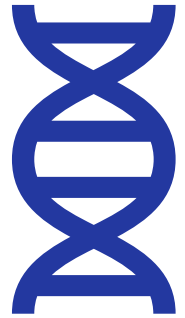
AI is becoming more intelligent each and every day.

We need to think about AI from the following perspectives:

Security

Privacy

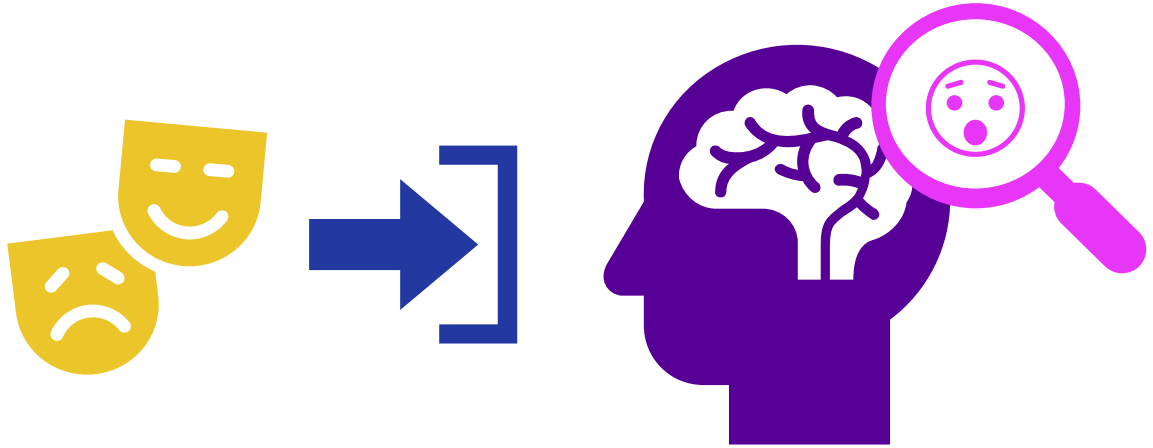
Legal



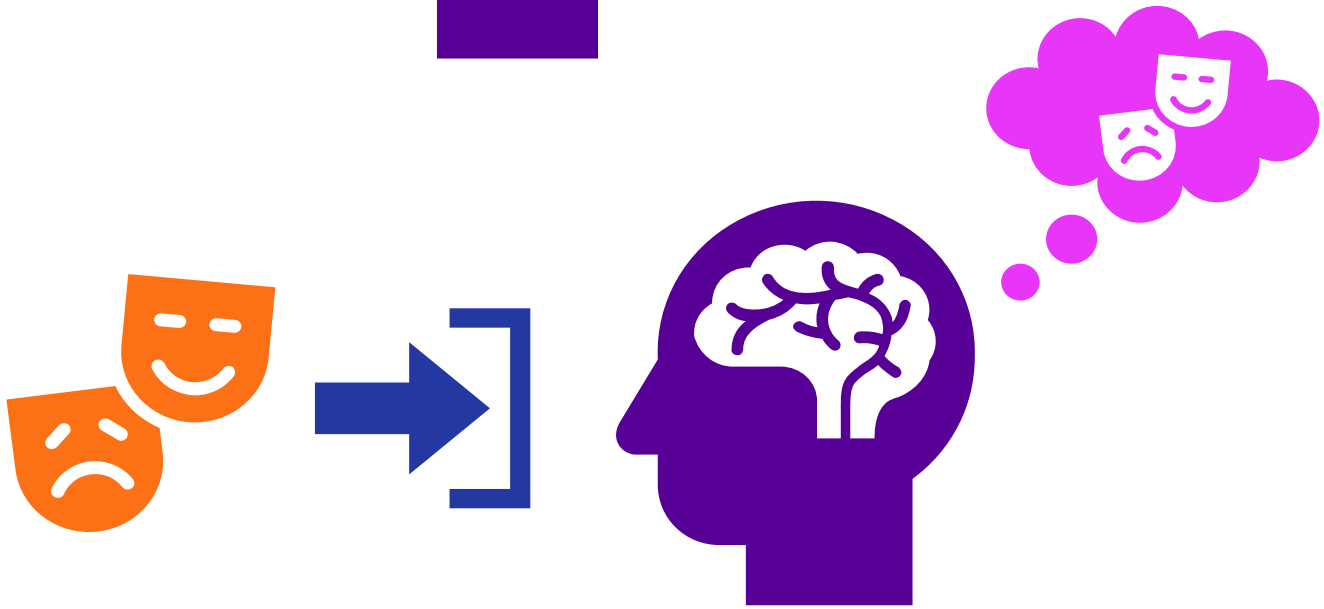
Ethical

Can the Human Brain be Hacked?

CEREBRAL SPYWARE



MENTAL MALWARE



Machine Learning

Machine learning is the process by which **AI systems learn from large sets of data to build models and find patterns that will help it make decisions and respond independently** (i.e. with little to no human guidance).

With every data point added to a network, **embedded AI can continue to refine itself, learning variations and deciphering information**.

Deep Neural Networks

Deep neural networks (DNN) are composed of deep learning **algorithms** designed to mimic the human brain. These algorithms **perform the same task over and over again**, learning and improving at each and every turn.

AI can use these algorithms to process large amounts of data and ultimately solve problems. **The more it learns, the stronger it becomes.**

And today, **we are producing – and sharing – more data than ever.**

A New Type of PII

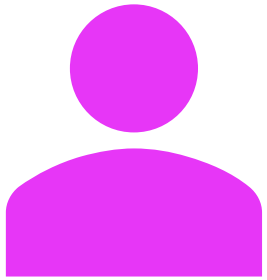
Sharing information about ourselves – not just who we are, but **what we say, what we do, what we watch and for how long** – gives AI more data to learn from, and unfathomable potential to **hack the human brain.**

per·son·al·ly i·den·ti·fi·a·ble in·for·ma·tion
/ˈpərs(ə)nəlē/ˌīˌden(t)əˈfīəb(ə)l,īˈden(t)əˌfīəb(ə)l/ˌinfərˈmāSH(ə)n/

information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Listen and Learn

Voice data offers AI a treasure trove of information about ourselves. **Commands** are used to **trigger voice-activated AI**, however after a **"wake word"** is provided, this technology can **learn more about us beyond just the questions we ask.**



Identity

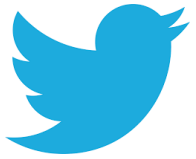
Emotion

Health

Social Media

AI also plays an important role in **social media.**

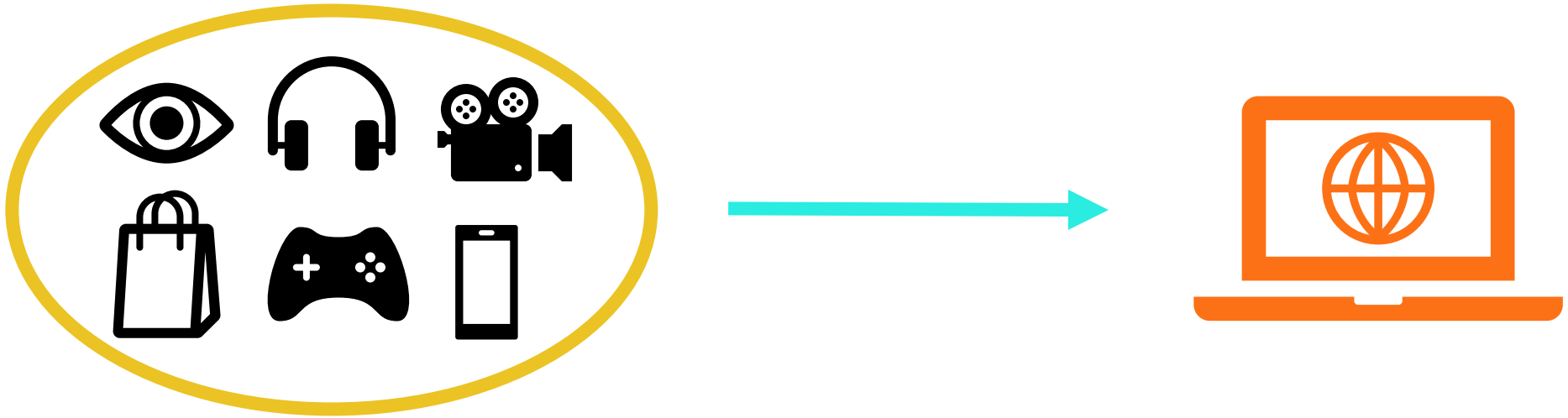
At **Facebook**, machine learning helps tailor users' News Feeds, determine which ads they see, and classify photos and video content in real-time, among other uses.



On **Twitter**, timelines are driven by an algorithm that shows users the most relevant content for them based on the author and Tweets that the user has found engaging in the past.

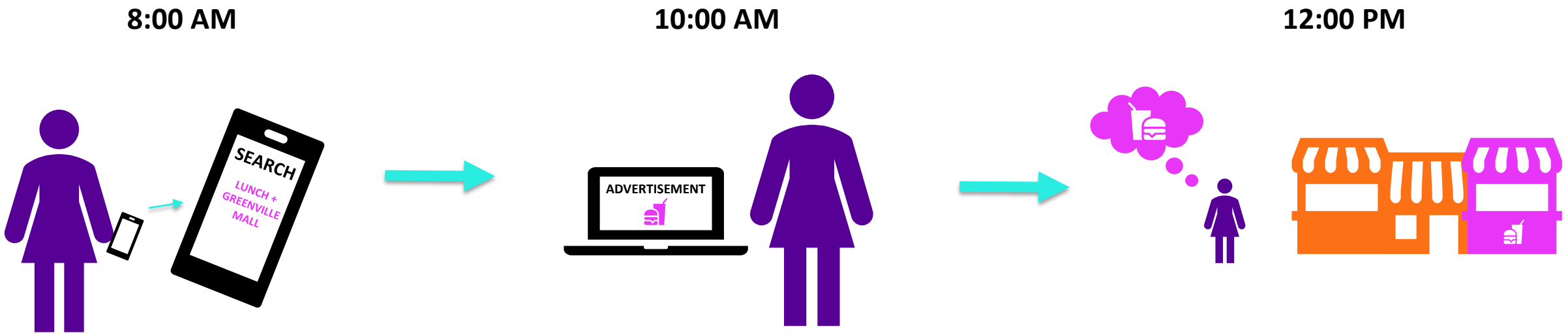
Leveraging Information for Tailored Targeting

Advanced AI could one day take **all of the personally identifiable information we produce** – our conversations, our search history, what we watch, what we buy, the time we spend reading an article, etc. – and convert it to **data** that can be used to **tailor our online experience.**



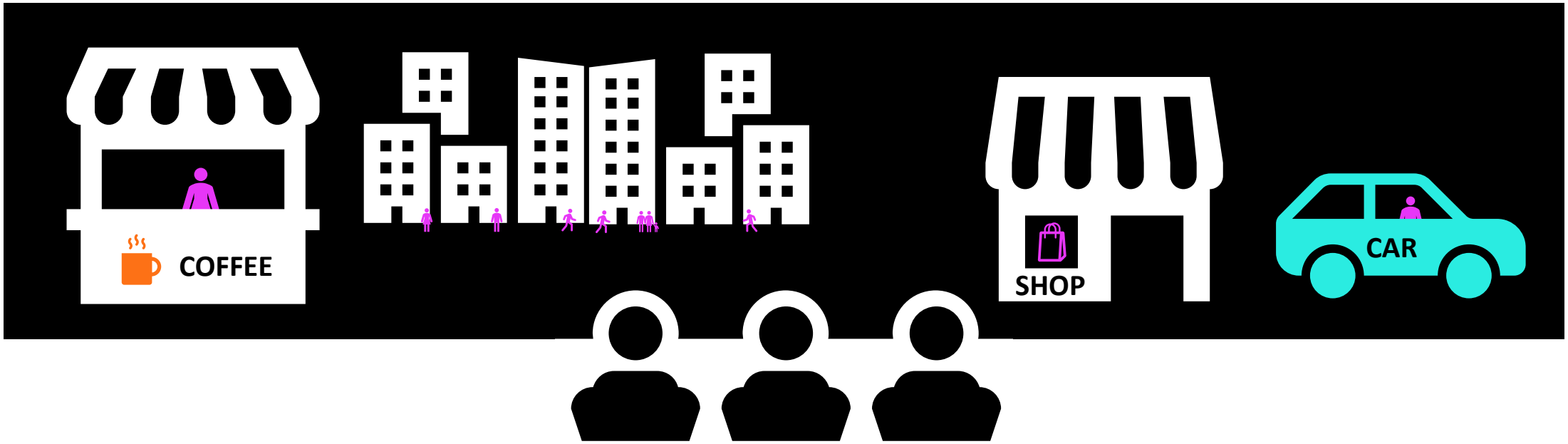
Mental Malware in Practice

We need to think not only about the **security** of the human brain, but also how the sharing of **private information we produce** can be used to **engineer influence** on what we buy, what we watch, what we read, and a host of other **"independent" decisions** we make.



From Product Placement…

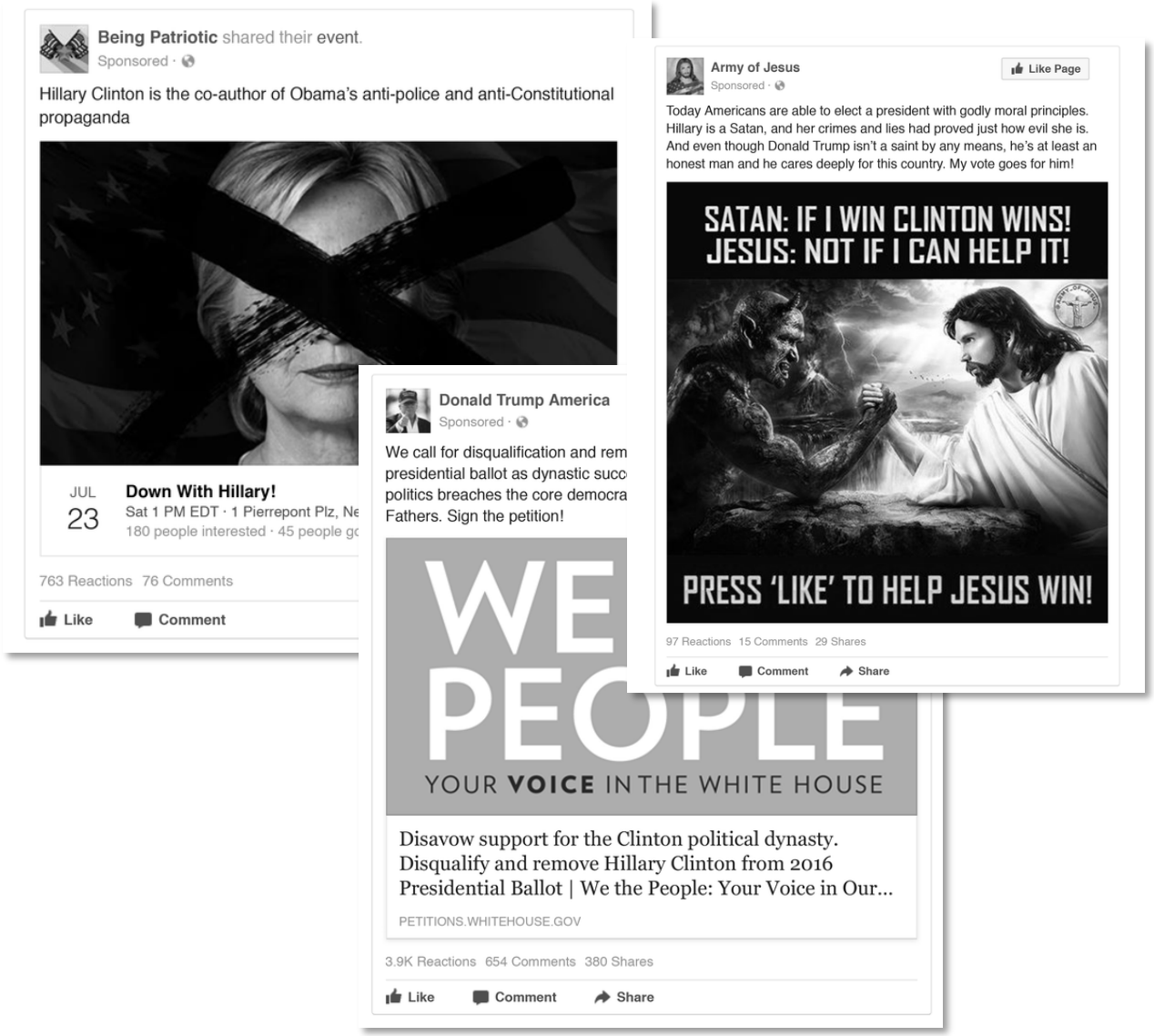
Product placement has historically been a mainstay of advertising…and one of the most well-known forms of **mental malware.**



…to Presidential Elections

But **convincing people to buy a product** is not very different from **changing the way they cast a ballot.**

And today, individuals and organizations **seeking to influence have more information about us at their disposal than ever before.**



Adversaries and AI

Every **interaction** we have with **Internet-connected technology produces data** – information that could be leveraged by malicious actors to:

Gather intelligence about individuals' private conversations, purchases, and browsing history

Target users with advertisements and posts that include untrue or inflammatory content

Extort individuals for confidential information or compensation

Covertly sew discord among the general public

Changing the World Through Code

Hacking the human brain isn't necessarily a bad thing. For example, in the health care sector, AI could eventually be perfected enough to **help** us:

Diagnose behavioral and emotional disorders

Recognize brain changes caused by Alzheimer's years before the first signs appear

Identify potentially destructive behaviors

Treat symptoms of depression and other issues

Building Cybersecurity into AI

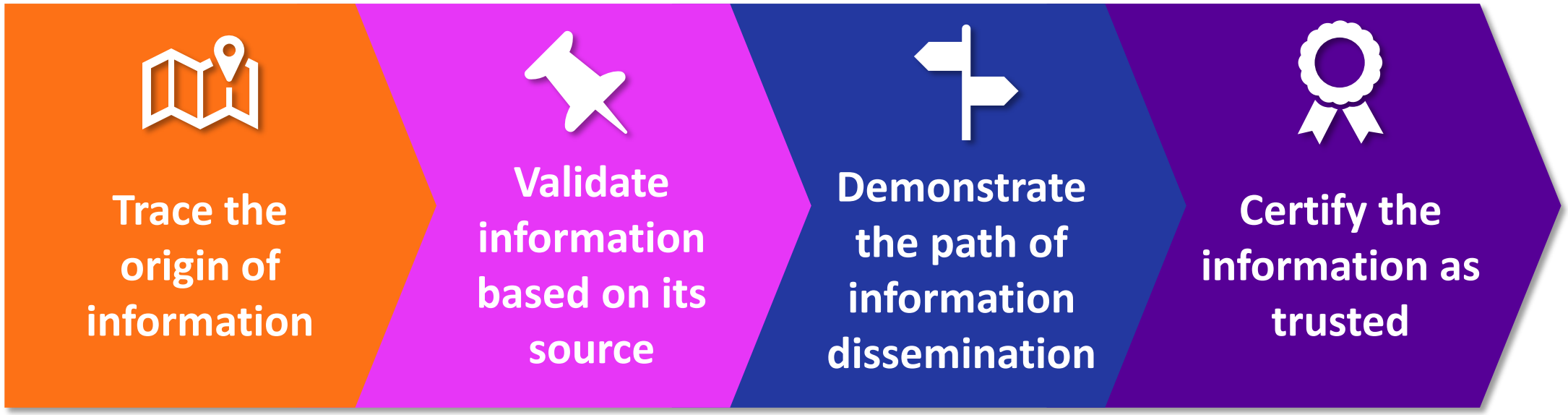
One of the biggest conversations in tech has been around the **use of AI in cybersecurity** – how can we leverage this tool to deploy stronger safeguards and better detect and defend against intrusions.

*But are we building **cybersecurity** into the foundation of **AI-based technology?***

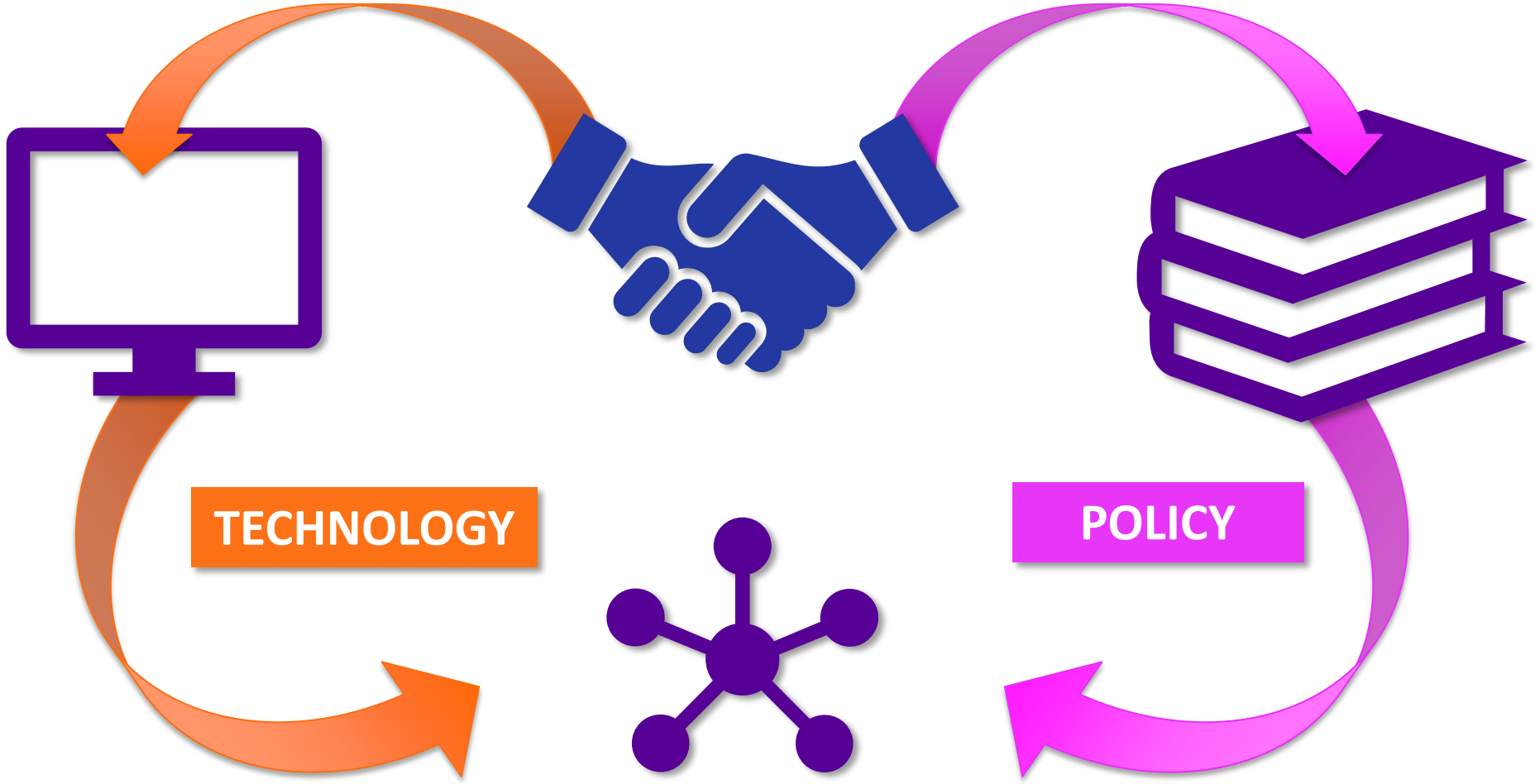
Weaknesses in AI technology could be exploited by malicious actors. For example, **deep neural networks could be flooded with data** that stalls machine learning process with contradictory information – **tricking AI systems and even hindering future advancement.**

Combatting Misinformation: Blockchain for Good

Blockchain can help stymie the spread of AI-driven mental malware. Through blockchain, we can:



Importance of Partnerships



Apply

When you encounter new applications for AI in your field, ask yourself:

How is the technology protected from malicious actors?

How will the data collected be used?

Could any information that is collected be used against users?

What are the broader implications of using this new technology?

RSAConference2019

Anthony J. Ferrante

Global Head of Cybersecurity and Senior Managing Director

FTI Consulting

@FTICyber

ajf@fticonsulting.com