Medical Data Privacy and Ethics in the Age of Artificial Intelligence

Lecture 1: Introduction and Overview

Zhiyu Wan, PhD (wanzhy@shanghaitech.edu.cn)
Assistant Professor of Biomedical Engineering
ShanghaiTech University

February 19, 2025

privacy
Search term

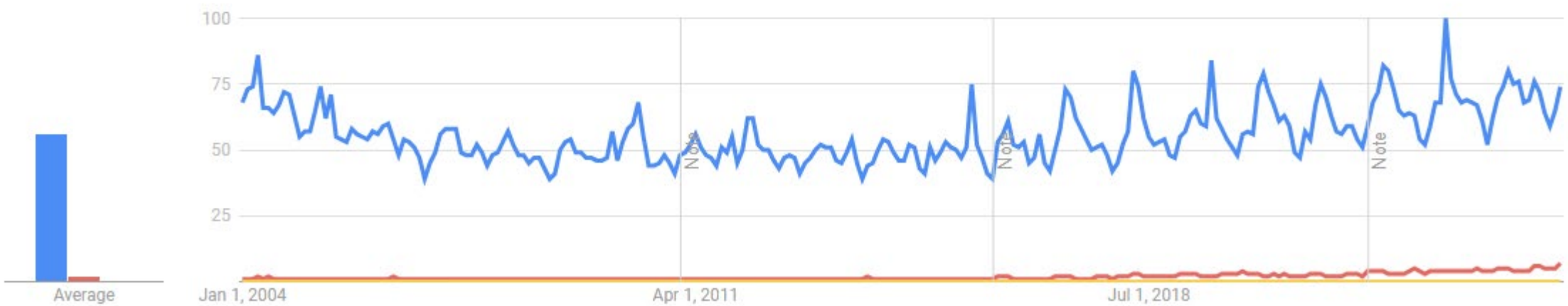
Data Privacy
Search term

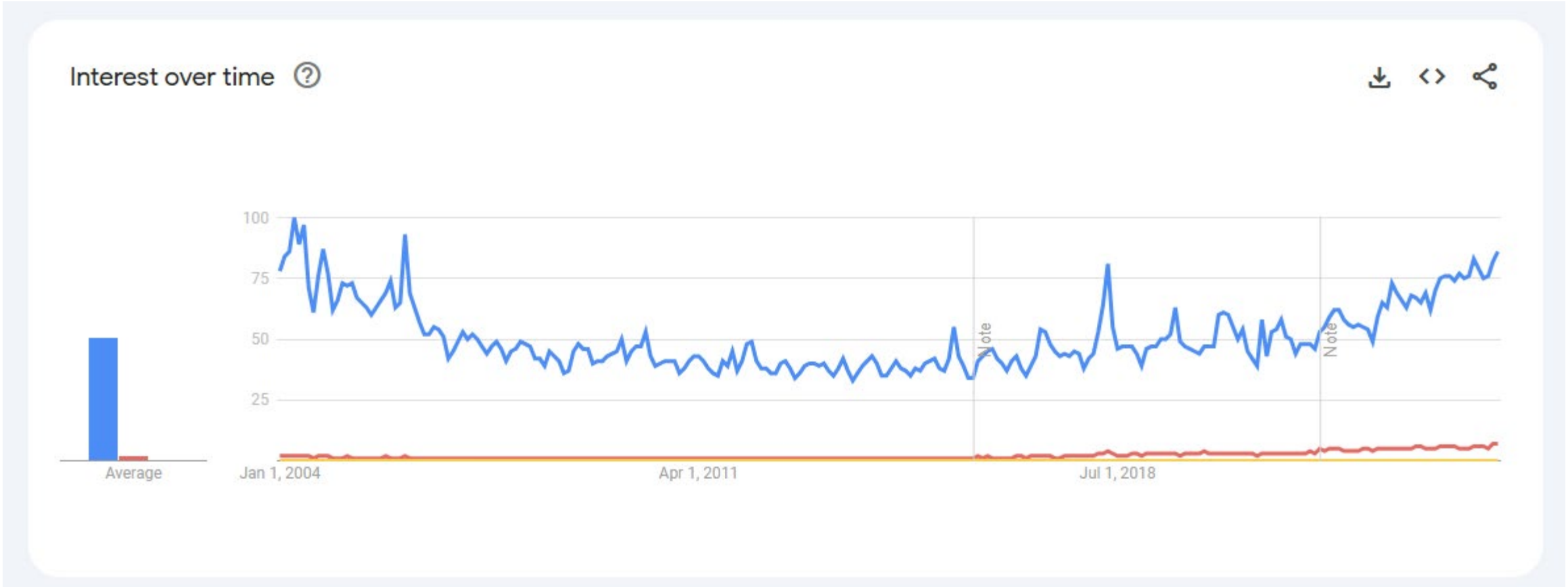
Medical Data Priv...
Search term

+ Add comparison

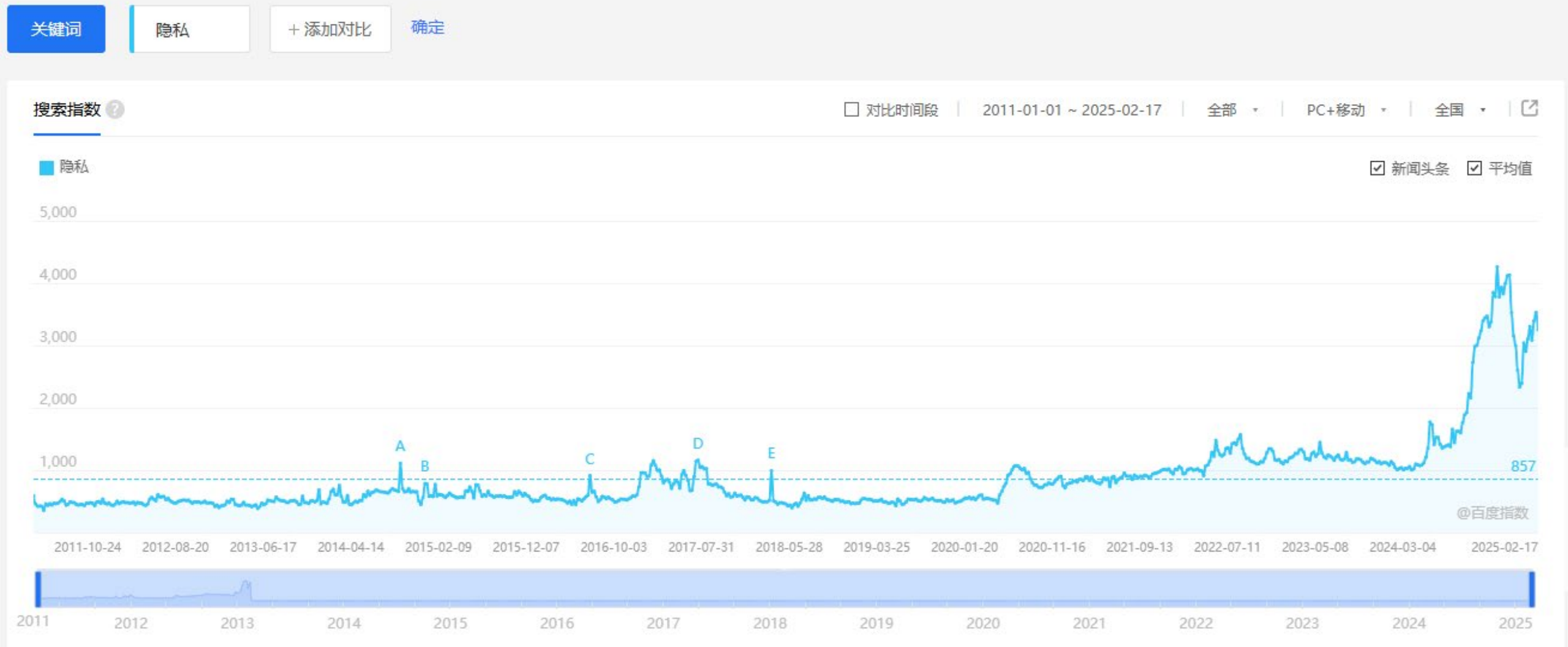
United States | 2004 - present | All categories | Web Search

Interest over time




Interest over time
100
75
50
25
Note
Note
Average
Jan 1, 2004
Apr 1, 2011
Jul 1, 2018

Worldwide



https://index.baidu.com/

地域分布 隐私

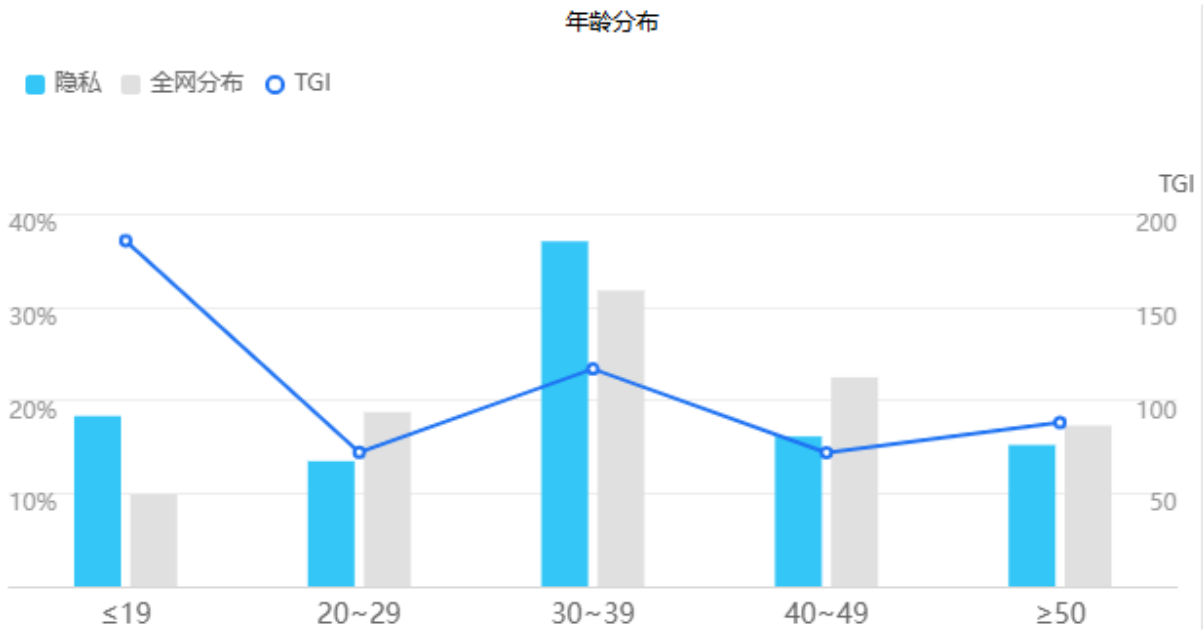
2013-07-01 ~ 2025-02-17 | 全部

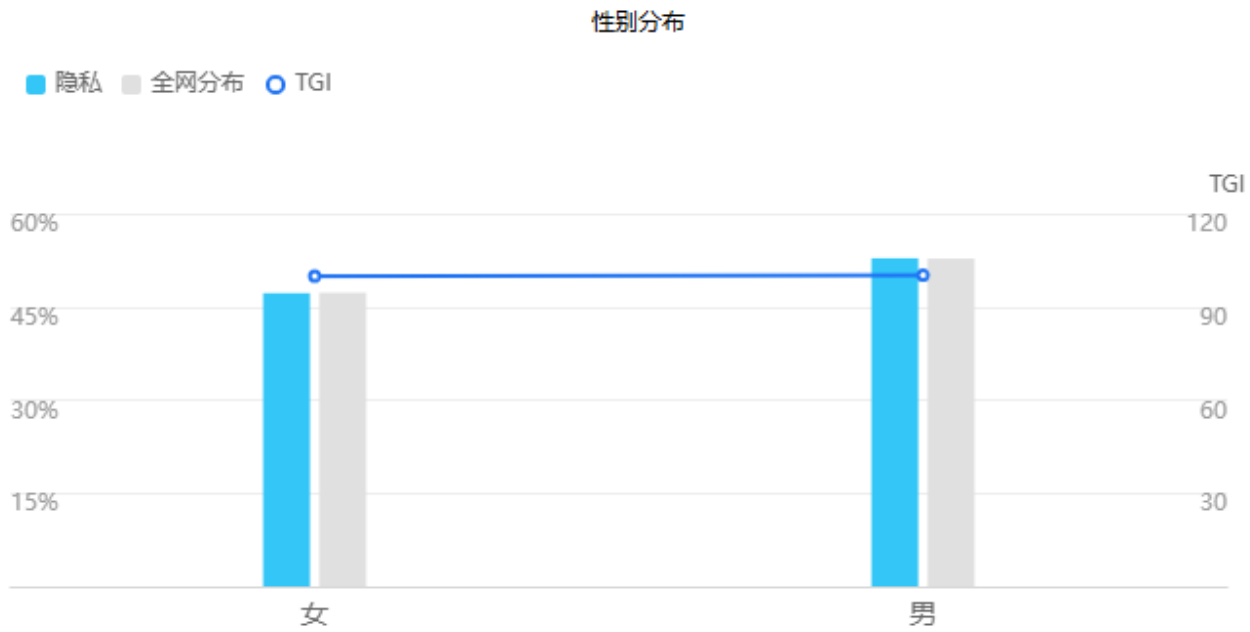
省份 区域 城市

1. 北京
2. 上海
3. 成都
4. 广州
5. 重庆
6. 深圳
7. 杭州
8. 天津
9. 武汉
10. 郑州

人群属性

2025-01-01 ~ 2025-01-31





ChatGPT
Search term

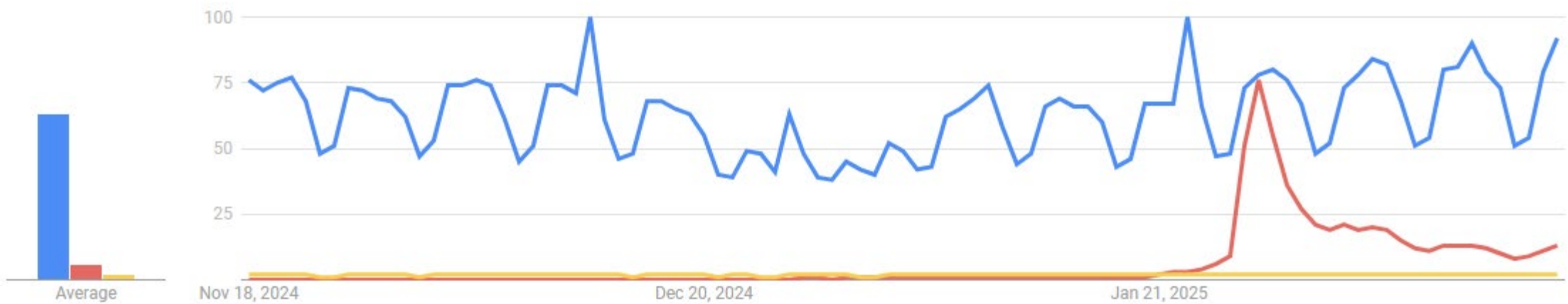
DeepSeek
Search term

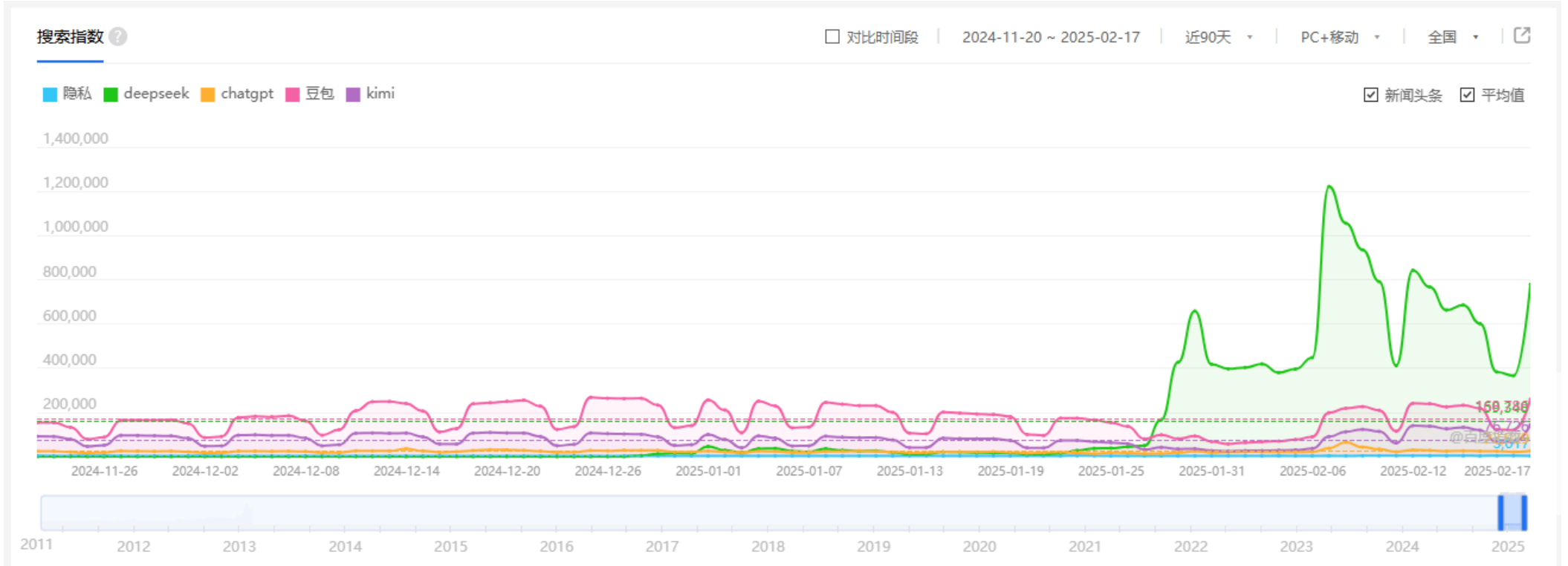
Privacy
Search term

+ Add comparison

Worldwide | Past 90 days | All categories | Web Search

Interest over time





搜索指数概览

关键词	整体日均值	移动日均值	整体同比	整体环比	移动同比	移动环比
隐私	3,017	2,927	162% ↑	-20% ↓	180% ↑	-20% ↓
deepseek	159,348	63,606	-	-	-	-
chatgpt	22,939	15,070	-23% ↓	16% ↑	-18% ↓	22% ↑
豆包	168,786	58,868	4888% ↑	118% ↑	4033% ↑	106% ↑
kimi	76,726	17,353	11091% ↑	43% ↑	3879% ↑	38% ↑

ⓘ 数据更新时间：每天12~16时，受数据波动影响，可能会有延迟。

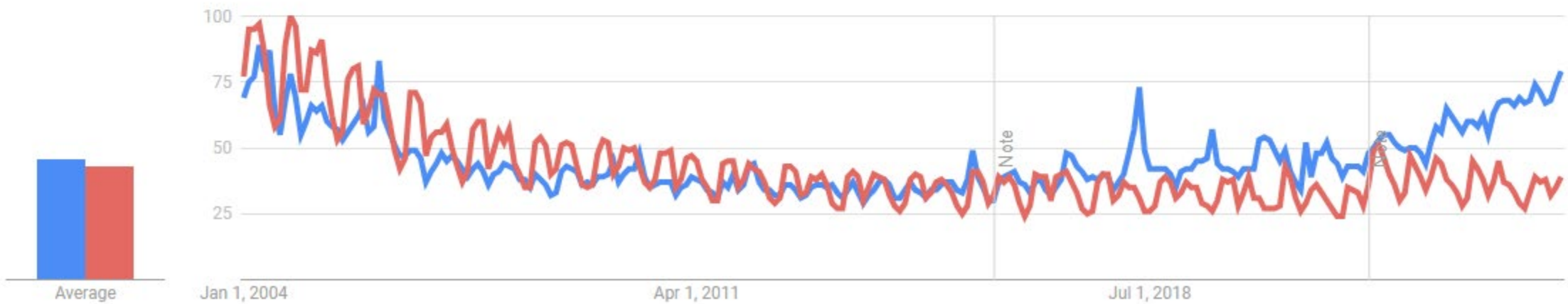
Privacy
Search term

Ethics
Search term

+ Add comparison

Worldwide | 2004 - present | All categories | Web Search

Interest over time



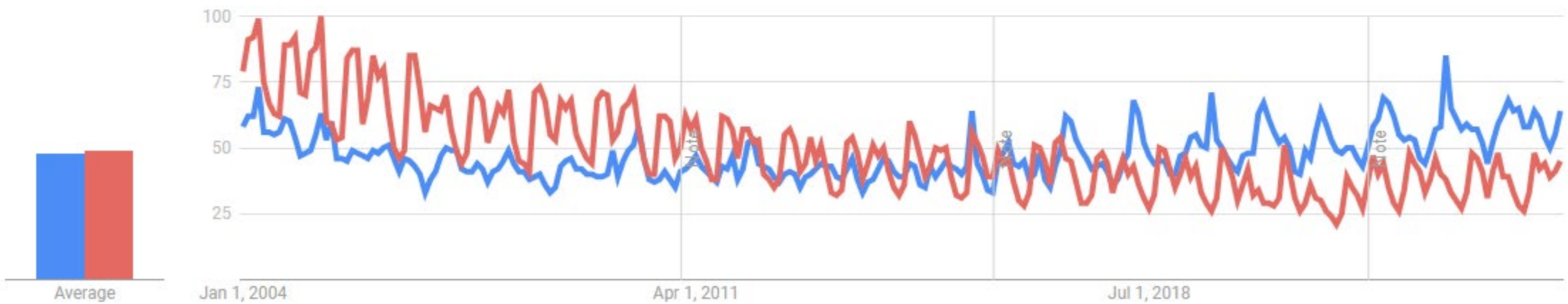
Privacy
Search term

Ethics
Search term

+ Add comparison

United States | 2004 - present | All categories | Web Search

Interest over time

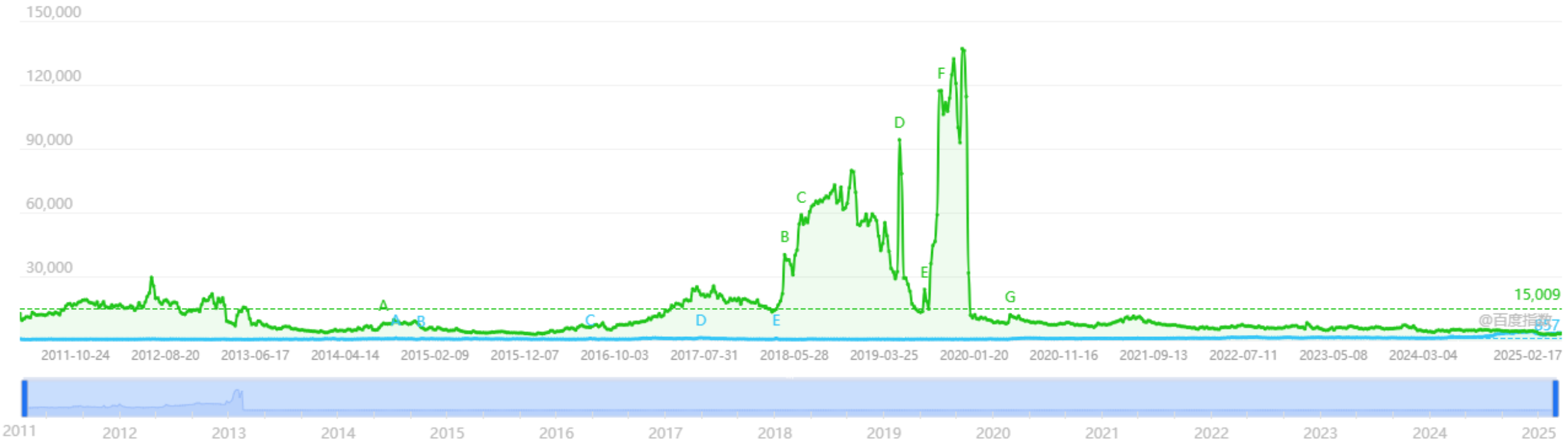


搜索指数

对比时间段 | 2011-01-01 ~ 2025-02-17 | 全部 | PC+移动 | 全国

隐私 伦理

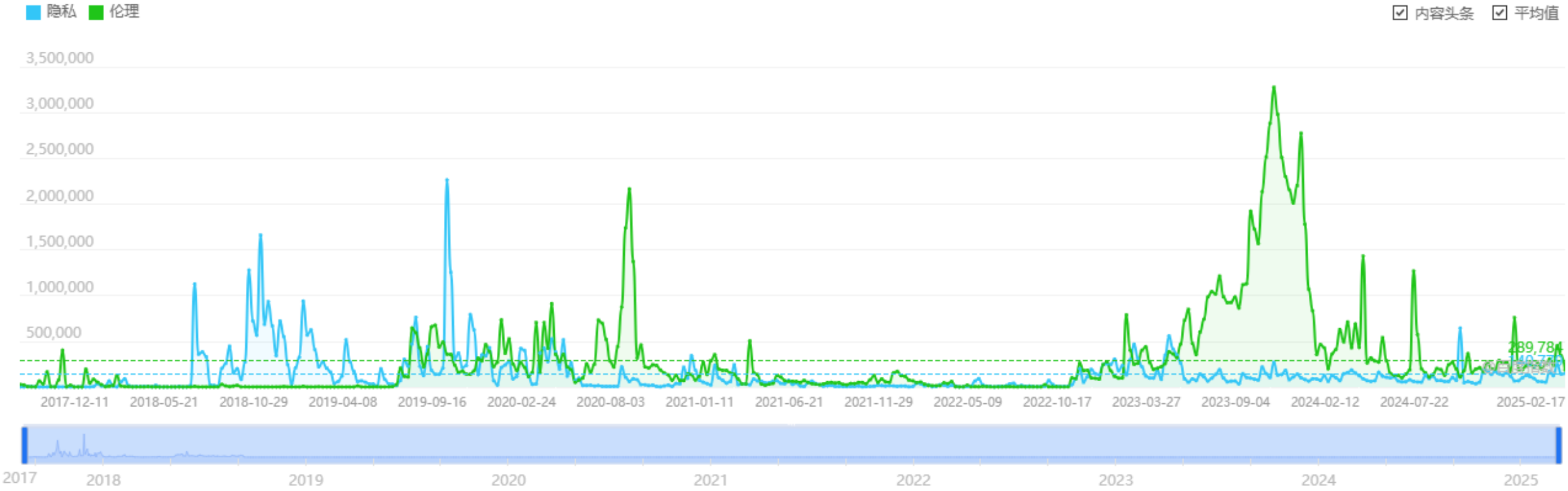
新闻头条 平均值



搜索指数概览

关键词	整体日均值	移动日均值	整体同比	整体环比	移动同比	移动环比
隐私	854	686	-	-	-	-
伦理	15,025	12,380	-	-	-	-

资讯关注 资讯指数 2017-07-03 ~ 2025-02-17 | 全部 | 全国



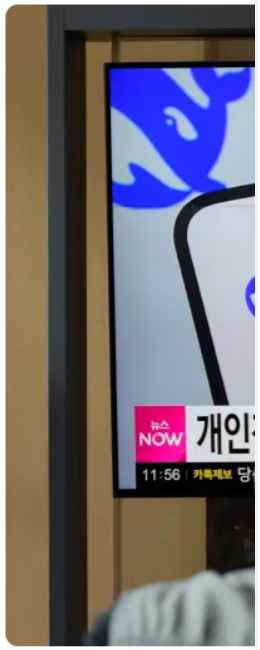
资讯指数概览

关键词	日均值	同比	环比
隐私	140,760	-	-
伦理	290,007	-	-

ALJAZEERA

政治 | 商业与经济

韩国将 Dee
隐私审查



人们在2025年2月17日的韩国首

2025年2月17日

韩国已暂停下载 Dee
的隐私标准进行审查

韩国隐私监管机构周
谷歌 Play 的本地版本
个人数据保护规则。

观 风闻

输入感兴趣的内容

我问：DeepSeek你怎么看
个人数据使用问题的说明。

guan_15823883882875

它（DeepSeek）回答我如下：

意大利隐私监管机构Garante对深度求索（Deep
隐私保护日益严格的监管趋势，同时也凸显了跨
以下几个角度分析：

1. 国际数据隐私监管趋严的背景。

GDPR框架下的合规要求：作为欧盟成员国，意大
（GDPR）。GDPR对个人数据的收集、存储、跨
性、透明性和必要性。

对非欧盟企业的重点关注：近年来，欧盟监管机
为敏感，尤其在数据主权和跨境传输方面。例如，
决、对TikTok的多次调查等均体现了这一趋势。

2. 深度求索可能面临的挑战。

数据本地化与跨境传输：Garante特别关注数据是
的评估。若企业需将欧盟用户数据传输至中国，
充分性认定等），而目前欧盟尚未承认中国具备

透明性与用户知情权：Garante要求说明数据收集
需明确告知用户数据处理方式并获得有效同意。
其符合“最小必要”原则。

3. 中欧数据治理的潜在摩擦点。

数据主权与信任问题：欧盟近年来推动“数字主
据安全法》《个人信息保护法》虽在立法层面与
权限等问题上仍存在互信缺口。

地缘政治的影响：尽管数据合规本质上是法律问
审查。例如，此前意大利曾短暂禁用ChatGPT，

腾讯：微信接入De
和隐私，仅整合公

澎湃新闻记者 范佳来

2025-02-16 13:03 来源：澎湃新闻 · 10%公司 >

微信回应灰度测试接入DeepSeek。

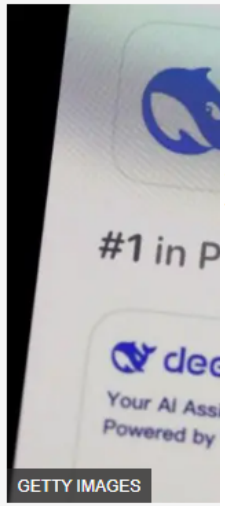
2月16日，澎湃新闻记者获悉，微信
日正式灰度测试接入DeepSeek。被
“AI搜索”字样，点击进入后，可免
化的搜索体验。

对于部分获得测试资格的用户，在聊
入口，点击后出现输入框，并有“快

腾讯方面表示，腾讯多个产品正在探
元宝等，为用户提供更丰富的体验和

对于微信此番接入DeepSeek，外界
搜索。通过微信AI搜索，可以整合公
等内容，以往的公众号历史文章、视
新发现，对于腾讯而言，这无疑将进
DeepSeek接入微信，也意味着更大

DeepSe
员为何对



DeepSeek在美国的应

汤姆·葛肯 （Tom Ger

BBC科技记者

2025年1月29日

澳洲科学部长艾德·胡
私担忧的西方政府高层

中国科技企业，如华为
并引发对个人数据可能

美国总统唐纳德·特朗
乎并未暗示它对国家安

然而，胡西克在周二接
许多未解答的问题，包
这类问题需要仔细权衡

首页 国际 中国

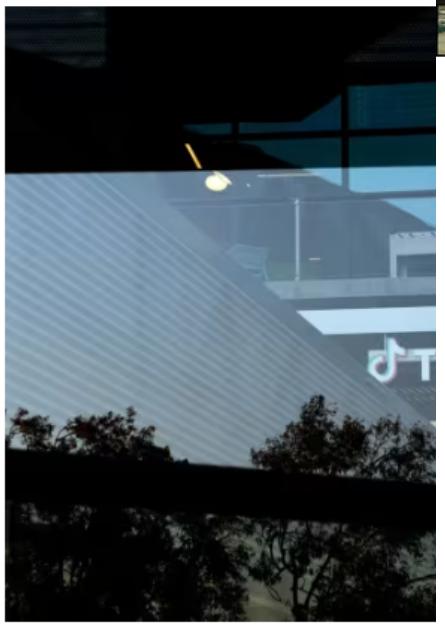
TikTok面临美国
隐私权的新指控

美国FTC周二建议对TikTok提起民
儿童网络隐私权的法律。

Dave Michaels / Georgia Wells

更新于 2024年6月19日 08:20 CST

分享



TikTok发言人说，一年多来，该公司一直在与F

图片来源：BING GUAN/BLOOMBERG NEWS

美国联邦贸易委员会(Federal Trade Co
起民事诉讼，指控其违反了一项旨在保

FTC称一直在调查TikTok是否遵守了早
TikTok可能有新的违反该项法律的行为

该公司本周请求最高法院驳回在美国禁止该应用的法案。 BING GUAN/BLOOMBERG

俄罗斯因TikTok未删除违禁内容而对其处以罚款。由于担心该应用被用于传播外国影响力，罗马尼亚的总统选举结果被推翻。在一名青少年因与另一名青少年在网上争吵将其刺死后，阿尔巴尼亚禁止使用TikTok一年。

“要么TikTok保护阿尔巴尼亚的儿童，要么阿尔巴尼亚保护自己的儿童不受TikTok的伤害，”该国总理埃迪·拉马在X上表示。

这都只是上个月发生的事。

美国约有1.5亿人使用TikTok应用程序，本周，TikTok及其中国母公司字节跳动请求最高法院废除一项法律，该法律将迫使TikTok出售或禁用该应用程序。

近年来，TikTok在世界各地受到法律和政治审查，至少在20个国家面临全面或部分禁令，这些政府对其与中国的关系及其广泛的影响力，尤其是在年轻人中的影响力感到警惕。

Forbes

FORBES > INNOVATION > CYBERSECURITY

ChatGPT-4o Is Wildly Capable, But It Could Be A Privacy Nightmare

Kate O'Flaherty Senior Contributor
Kate O'Flaherty is a cybersecurity and privacy journalist.

Follow

0

May 17, 2024, 06:04am EDT

OpenAI has launched ChatGPT-4o and it comes with impressive capabilities. ChatGPT-4o is much more human-like than previous iterations, able to solve equations, tell bedtime stories and identify emotions from visual expressions.

But as a privacy journalist, I find ChatGPT-4o concerning. AI needs vast amounts of data to operate and just using chatbots requires you to enter a bunch of information about yourself. This means you are relying on ChatGPT owner OpenAI to keep your data safe and protect your personal information.

ChatGPT maker OpenAI has launched ChatGPT-4o and it comes with impressive capabilities. But it also ... [+] NURPHOTO VIA GETTY IMAGES

Reuters

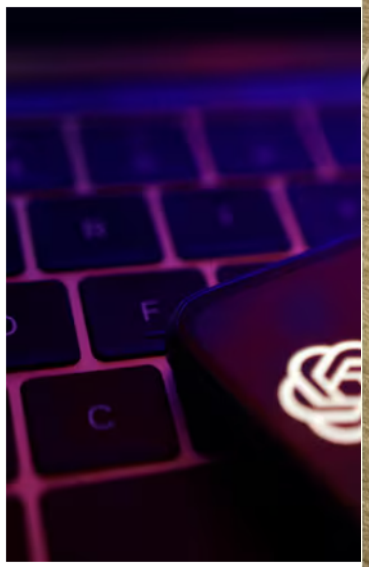
World Business Markets Su

Home → Tech

Italy fines OpenA rules breach

By **Elvira Pollina** and **Alvise Armellini**

December 21, 2024 4:51 AM GMT+8 · Updated



OpenAI logo is seen in this illustration taken May 20, 20

Summary Companies

- Italian data regulator fines OpenAI 15
- Company says decision disproportiona
- Watchdog briefly banned ChatGPT las
- Open AI ordered to launch media cam

MILAN, Dec 20 (Reuters) - Italy's data pro million euros ($15.58 million) after closing artificial intelligence application.

The fine comes after the authority found C having an adequate legal basis and violat obligations towards users".

Apple priva

By Chr

Image: José

If you

Appl iPho will a relea build

This avail The can

Copy link
Email
X (Twitter)
Bluesky
Facebook
27

THE CONVERSATION

Academic rigor, journalistic flair

Arts + Culture Economy Education Environment + Energy Ethics + Religion Health Politics + Society Science + Tech Podcasts

Apple insists its ChatGPT tie-up will protect users' privacy: here are the questions it must answer first

Published: June 14, 2024 12:31pm EDT

Apple CEO Tim Cook and software engineering head Craig Federighi unveiling new AI features at the Apple Worldwide Developers Conference. EPA

Apple, a company known for its longstanding commitment to user privacy, has received flak since unveiling its artificial intelligence (AI) strategy at its Worldwide Developers Conference on June 10. This relates to the centrepiece of Apple Intelligence, which gives users access to OpenAI's powerful generative AI tool, ChatGPT.

NEWS MEDICAL LIFE SCIENCES

MEDICAL HOME | LIFE SCIENCES HOME | Become a Me

About | News | Health A-Z | Drugs | Medical Devices | Interviews

Advances in artificial intelligence threaten privacy of people's health data

Download PDF Copy

January 2019

Reviewed by James Ives, MPsych Jan 4 2019

Advances in artificial intelligence have created new threats to the privacy of people's health data, a new University of California, Berkeley, study shows.

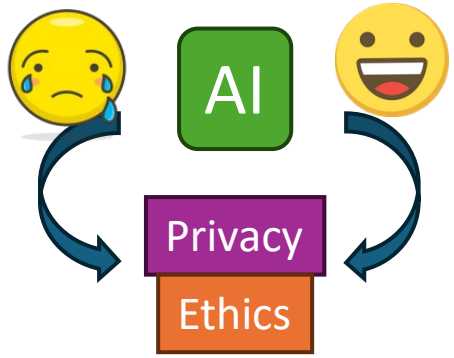
Led by UC Berkeley engineer Anil Aswani, the study suggests current laws and regulations are nowhere near sufficient to keep an individual's health status private in the face of AI development. The research was published Dec. 21 in the *JAMA Network Open* journal.

The findings show that by using artificial intelligence, it is possible to identify individuals by learning daily patterns in step data, such as that collected by activity trackers, smartwatches and smartphones, and correlating it to demographic data.

The mining of two years' worth of data covering more than 15,000 Americans led to the conclusion that the privacy standards associated with 1996's HIPAA (Health Insurance Portability and Accountability Act) legislation need to be revisited and reworked.

"We wanted to use NHANES (the National Health and Nutrition Examination Survey) to look at privacy questions because this data is representative of the diverse population in the U.S.," said Aswani. "The results point out a major problem. If you strip all the identifying information, it doesn't protect you as much as you'd think. Someone else can come back and put it all back together if they have the right kind of information."

"In principle, you could imagine Facebook gathering step data from the app on your smartphone, then buying health care data from another company and matching the two," he added. "Now they would have health care data that's matched to names, and they could either start selling advertising based on that or they could sell the data to others."



Microsoft forms new coalition for AI in healthcare

By Elly Yates-Roberts on 17 January 2022

Microsoft has created the Artificial Intelligence Industry Innovation Coalition (AI3C) to drive the use of artificial intelligence (AI) in healthcare by providing recommendations, tools and best practices.

Member organisations include The Brookings Institution, Cleveland Clinic, Duke Health, Intermountain Healthcare, Novant Health, Plug and Play, Providence, UC San Diego, and University of Virginia.

"The goal of the newly created AI3C is to establish a pragmatic coalition with public and private organisations to advance health by identifying and addressing significant societal and industry barriers," said Patty Obermaier, vice president of US health and life sciences at Microsoft. "I am excited about the launch of AI3C and working with its distinguished board as we continue the momentum towards serving the needs of patients and communities through AI innovation."

According to Microsoft, the AI3C board will work to "create AI solutions for positive societal and healthcare outcomes, identify and set the AI strategy and vision for a variety of projects, and track the success of AI adoption in the industry".

The coalition will use AI to solve economic and industrial challenges, address digital skills and employability and improve data privacy. It will also accelerate AI innovation and adoption by showcasing emerging AI tools, collating use cases, best practices and research feedback, and preparing students for careers in AI and data science.

https://www.news-medical.net/news/20190104/Advances-in-artificial-intelligence-threaten-privacy-of-peoples-health-data.aspx

Welcome to Medical Data Privacy and Ethics in the Age of Artificial Intelligence

- You're sitting in BME2133

- When: Wednesdays (Odd Week) & Fridays, 15:00-15:45, 15:55-16:40
- Where: SIST Building 1 Area A, Room 108

- Office Hours: Upon Request
- Teaching Assistant: Yuhang Guo
- Contact: wanzhy@shanghaitech.edu.cn

Goals of this lecture

- Know more about this course
  - Instructor
  - Objectives
  - Grading
  - Schedule
- Overview of the concepts
  - AI
  - Medical Data
  - Medical AI
  - Privacy
  - Medical Data Privacy
  - Ethics

- Hi! I'm Zhiyu Wan.
  - BEng, Automation. XJTU (Gifted Young)
  - MS & PhD, Computer Science, Vanderbilt
  - Postdoc, Biomedical Informatics, VUMC
- Faculty in Biomedical Engineering
- Health Information Safety and Intelligence Research Lab

  (https://zhiyuwan.com/hisir-lab/)
- Sample Research Areas
  - Genomic Data Privacy
  - Biomedical Data Anonymization
  - Synthetic Data Generation
  - Responsible AI
  - AI Ethics

2024 Nobel Prize Winners, Me, and the HISIR Lab

THE NOBEL PRIZE IN CHEMISTRY 2024

John M. Jumper

BS in Physics and Math from Vanderbilt University in 2007

Co-created AlphaFold that can be applied in Biomedicine: Drug discovery

Published *Power and Progress* which finds the way where technology could be harnessed for social goods

Simon Johnson

THE NOBEL PRIZE IN ECONOMIC SCIENCES 2024

HIS & IR

PhD in CS from Vanderbilt University in 2020

Attended NeurIPS 2022

THE NOBEL PRIZE IN PHYSICS 2024

Geoffrey E. Hinton

A keynote speaker at NeurIPS 2022

Godfather of AI, Deep Learning
Mentored Ilya Sutskever who co-created ChatGPT

Co-discovered microRNA, a type of genomic data, has genomic privacy

Gary Ruvkun

THE NOBEL PRIZE IN PHYSIOLOGY OR MEDICINE 2024

https://zhiyuwan.com/bme2133/

BME2133: Medical Data Privacy and Ethics in the Age of Artificial Intelligence

Schedule

Who / When / Where

Instructor: Zhiyu Wan
Teaching Assistant: Yuhang Guo
Semester: Spring 2025
Time: Wednesdays (Odd Week) & Fridays, 15:00-15:45, 15:55-16:40
Location: SIST Building 1 Area A, Room 108
Office Hours: Upon request, Location: BME Building, Room 228

Course Syllabus (PDF)(中文版)

First Day of Class: February 19, 2025

Description

" Medical Data Privacy and Ethics in the Age of Artificial Intelligence " is a specialized elective course for graduate students majoring in Biomedical Engineering and a foundational public course for Master of Engineering students in Biomedical Engineering. This course focuses on issues related to medical data privacy and ethics in the age of artificial intelligence (AI), with an in-depth exploration of privacy protection technologies, ethical dilemmas, and legal regulations surrounding medical data. The curriculum covers ethical challenges and privacy protection strategies that may arise during the collection, sharing, processing, and use of medical data. Through lectures, discussions, case studies, and project-based practice, this course aims to develop students' capabilities in designing intelligent medical systems and managing biomedical data. It helps students understand how to balance privacy protection with technological innovation in AI-driven healthcare data systems, and provides a sc in ethics, law, and technical practices for their future work in medical data processing.

The course comprises four fundamental modules: the first part introduces basic concepts and major challenges of and ethics in the age of artificial intelligence; the second part discusses social and legal approaches to protecting and ethics; the third part covers technical methods for privacy and ethics protection; and the fourth part applies th

Schedule

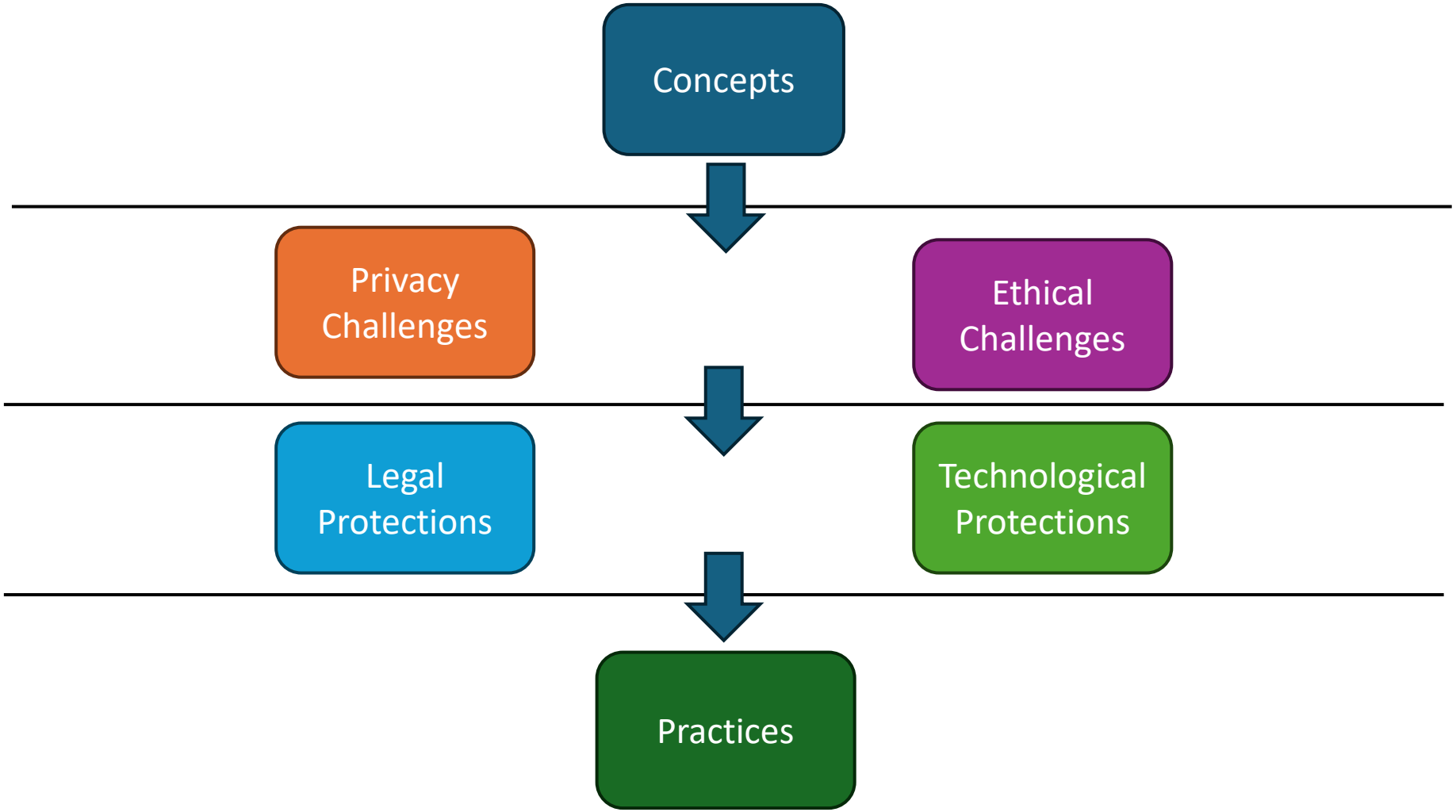
Week	Chapter	Teaching Contents	Reading	Assignment
Week 1, Wednesday Feb 19, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (a)(b)	The Role of Medical Data in the Age of AI. Concept of data privacy and its importance. Concept of ethics and morality and their importance.	/	
Week 1, Friday Feb 21, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (c)	AI ethics: machine morality and ethics, automation, and employment.	(Optional: 1.《信息科学技术伦理与道德》Chs.8-10. 2.《工程伦理》Ch.12. 3.《信息科学技术伦理与道德》Chs.3&4.)	
	II. Ethical Issues in Life Sciences, Medicine, and Informatics (a)	Research ethics: ethical guidelines for human and animal experiments and scientific research. Life sciences ethics: controversies arising from reproductive technology, genetic technology, stem cell research, etc. Medical ethics issues: abortion, euthanasia, public health issues, and medical ethics concerning special populations (infants, adolescents, psychiatric patients, etc.).		
		Information security and privacy issues: personal data breaches, surveillance	TBD (Optional:	

More to come (projects, homeworks, etc.) – links will be available from front page of website

Course Objectives

- After this course, you should be able to analyze data privacy and ethics risks from three non-exclusive perspectives:
  - *Data Detectives*: Understand how seemingly private information, can be discovered (or exploited) using automated strategies.
  - *Data Protectors*: Construct privacy protection technologies that provide formal computational guarantees of privacy in disclosed databases.
  - *System Builders & Policy Designers*: Develop a system or design a policy with built-in privacy mechanisms.

Course Modules



Expectations

- To Build a system: You are expected to be **competent** in an object-oriented programming language (Java, C++, Python, …)

- To analyze a dataset: You are expected to have a **working knowledge** of the Internet, word processing, and analysis tools (Python, R, Matlab, Excel, …)

- Reading & Writing in English.

Beyond Expectations

- You have experience in
  - information security (Cybersecurity Expert, Hacker)
  - data structures, algorithms, and statistics (Software Engineer, Statistician)
  - public policy and legal frameworks (Lawyer)

Instructional Pedagogy

- Inputs: Lectures, group discussions, case discussions, special topic seminars / guest lectures, massive open online courses (MOOCs).
- Deliveries (Outputs): In-class quizzes, reading summaries, homework assignments, and course research projects.
- Understanding-based, heuristic teaching approach aligned with international standards.
- Encourage active learning and research interests.
- The primary spoken language is Chinese, while written materials are primarily in English.

Grading

- This is a research-oriented course. There are no exams.
- A substantial portion of your grade will be based on your “final” project.

Criteria	% of Total Grade
Course Project	50%
Homework Assignments	30%
Reading Summaries	10% (+5%)
In-class quizzes	5%
Class Participation	5%
Total	100%

More details: https://zhiyuwan.com/bme2133/#grading

Homework Policy

- Please do your own homework.
- Do not plagiarize without proper attribution – not even in your reading summaries.
- You can use AI assistant. However, you may lose points due to lack of innovation.

Reading Summaries

More details: https://zhiyuwan.com/bme2133/#textbook

- There is no required textbooks for this course.
- Assigned readings will be available the lecture before it is due (at the latest).
- Your summaries should be no more than 2 pages in length.
- Summaries will be graded on a {A-, A, A+} scale
  - A- : You skimmed the reading and barely understood its meaning
  - A : You read the reading and provided a reasonable account of its contents
  - A +: You demonstrated critical reasoning and insight regarding the topic
- Submit summaries to wanzhy@shanghaitech.edu.cn before class.

More details: https://zhiyuwan.com/bme2133/#reading

Final Projects

- Your project should be an independent study on data privacy or ethics issues, with relationship to the area of biology, medicine, or health more generally (related to your own research areas preferred)
- You may design your own project or choose from a predefined set of topics (will be available on the course website later in the semester)
- Do not be afraid to discuss your project ideas with the instructor!

Sample Topics

- Access Control Frameworks for Distributed Medical Record Systems
- Surveillance of Electronic Medical Record Accesses for Suspicious Behavior
- Evaluation and Design of Privacy Technologies for Personal Health Records
- Finding & Relating Publicly Available Repositories of Person Specific Biomedical Information
- Building and Evaluating Clinical Text De-identification Tools
- Anonymization of clinical profiles / sets of diagnoses
- Applications of big data frameworks to sanitizing clinical data
- Applications of security frameworks (e.g., Blockchain)

Final Projects

Criteria	Due Date	% of Grade
Project Description: A one-pager that describes the project area and how you intend to address the research within the confines of this semester. This will be broken down into a several phases.	April 24	5%
Mid-term Project Proposal Presentation: Briefing for the class on project area and first phase of research. (No more than 5 minutes)	May 9	5%
Written Project Proposal Report: A summary of the progress you have made (No more than 4 pages).	May 8	10%
Final Project Presentation: Showcase of research methods and results. (No more than 15 minutes)	May 30 (Slides Due) + June 6	40%
Final Project Report: This will be in the form of a conference-style paper. It will summarize the research area, your methodology, experience, and contributions of your work.	June 13 (in lieu of final)	40%

Schedule

- Let’s look at the syllabus.

More details: https://zhiyuwan.com/bme2133-schedule/

Ethics (Feb 21, 28, March 5, 7)

- Ethical Issues in Biomedical Research and Informatics
  - AI ethics
  - Research ethics
  - Life sciences ethics
  - Medical ethics
  - Information security and privacy
- Ethical Issues in Data Sharing and Medical AI
  - Cybersecurity and crimes
  - Privacy challenges in data sharing
  - Data governance and data lifecycle management
  - Algorithmic fairness and bias
  - Patient informed consent

Quiz 1

(Picture from Brad's Slides)

The Law and regulations (March 7, 14)

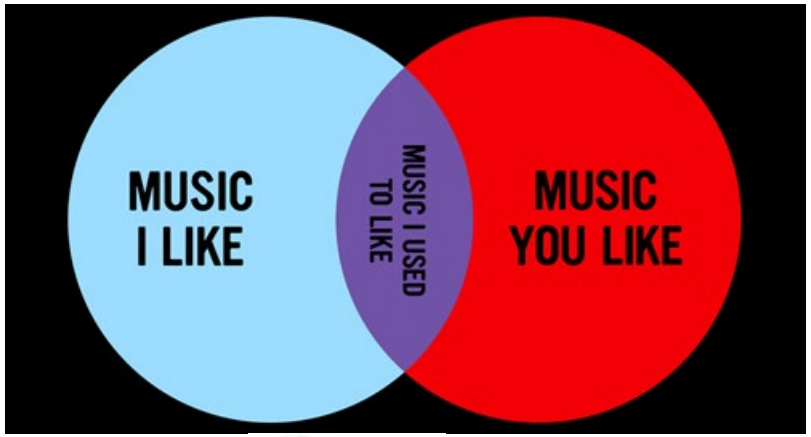
- The impact of international laws and regulations like HIPAA and GDPR on the impact of biomedical data.
- China's data security law and personal information protection law.
- Compliance requirements for medical data sharing.

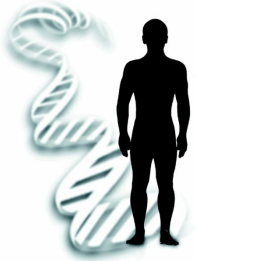
Quiz 2

(Picture from Brad's Slides)

Characteristics and Privacy Risks of Biomedical Data (March 19, 21, 28)

- Biomedical data:
  - Electronic health records
  - Natural language medical data
  - Genomic data
  - Medical image data
- Attack models:
  - Re-identification attacks
  - Membership inference attacks
  - Reconstruction attacks
- Risk Assessment Methods



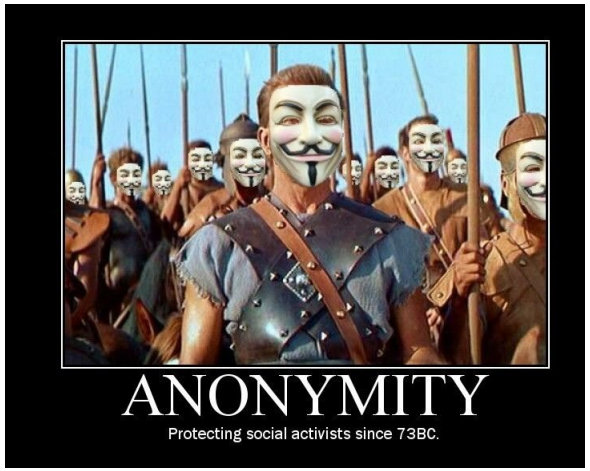


HW 1

(Pictures from Brad's Slides)

Common Privacy Protection Techniques for Medical Data (April 2, 4, 11, 16, 18)

- Data de-identification techniques
  - K-anonymization
- Game-theoretic models
- Differential privacy
- Access control and audit techniques
- Cryptographical methods
  - homomorphic encryption
  - secure multi-party computation
  - Encrypted hardware



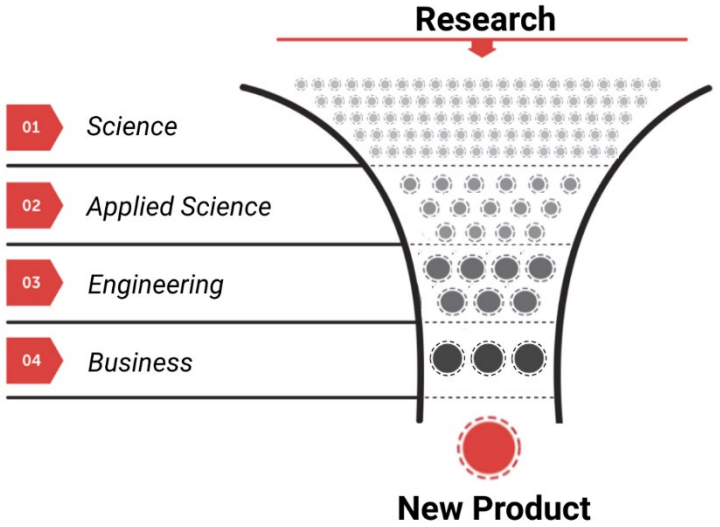
HW 2

HW 3a

(Pictures from Brad's Slides)

Advances in Frontier Technologies and Future Trends in Medical Data Privacy Protection (April 18, 25, 30, May 2)

- Federated learning
- Synthetic data generation
- Blockchain
- Future trends



HW 3b

(Picture from Brad's Slides)

Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare (May 2, 9, 14, 16, 23)

- Large Language Models & Generative AI
  - Introduction
  - Applications
  - Privacy issues
  - Fairness issues
  - Other ethical issues
  - Solutions and future directions

Project

Course Project Presentation (May 30, June 6)

- The students are in control
- You'll be graded by a committee of special reviewers

(Picture from Brad's Slides)

Introduction to AI

- **Definition of AI**: AI refers to the simulation of human intelligence in machines that are programmed to think, learn, and make decisions.

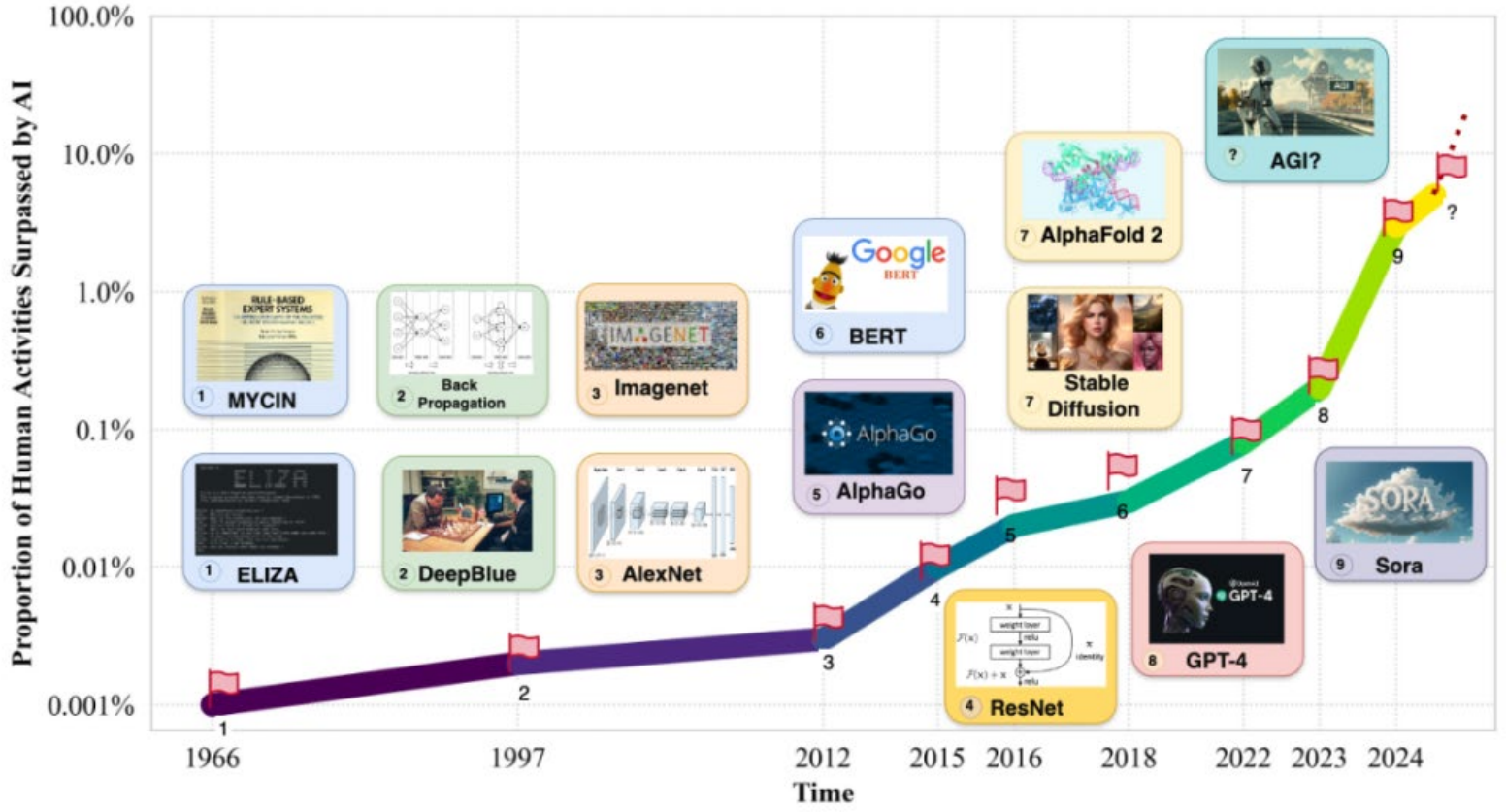
- **Types of AI**:
  - Narrow AI: Specialized in performing specific tasks.
  - General AI: Hypothetical, with abilities similar to human cognitive functions.

Development of AI

- **Early Development**: The origins of AI date back to the 1950s, with pioneers like Alan Turing and John McCarthy.

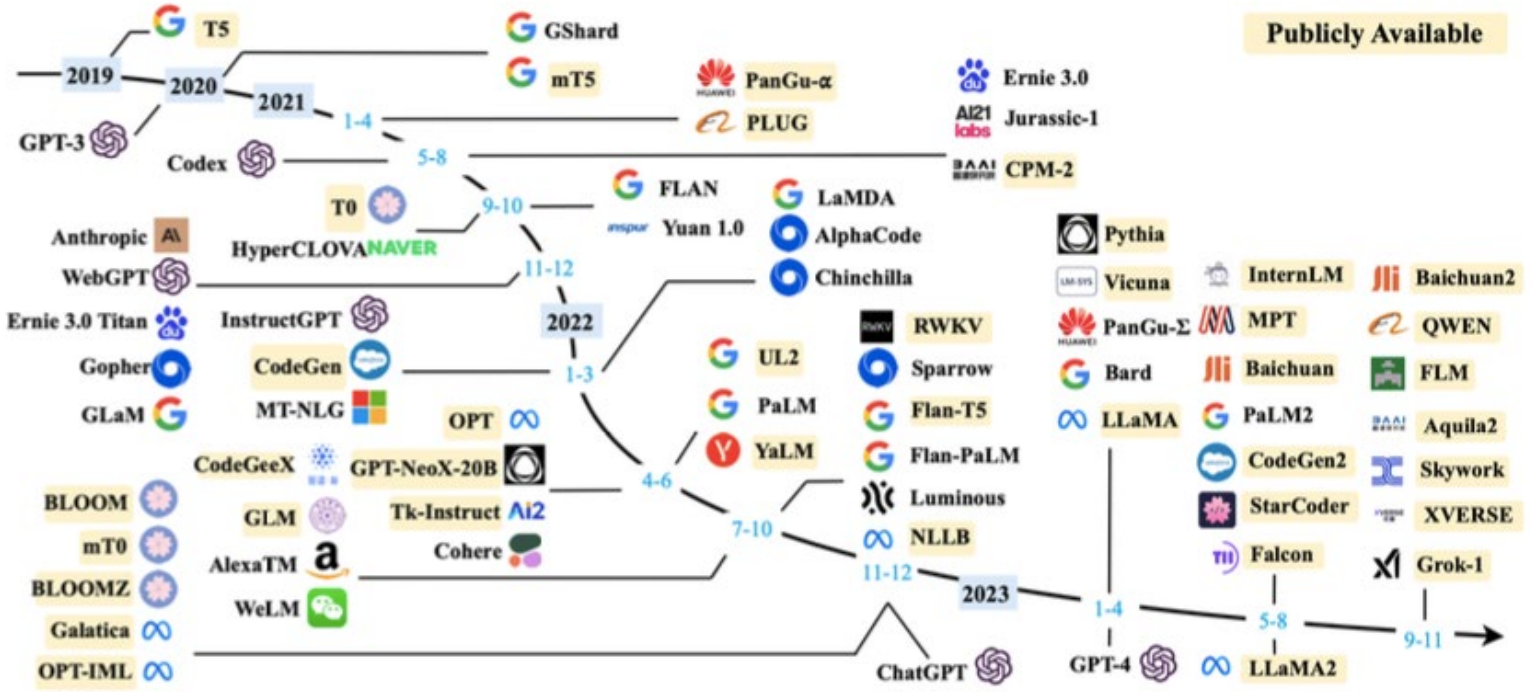
- **Advancements in Machine Learning**:
  - 1990s: Introduction of supervised and unsupervised learning.
  - 2010s: Emergence of deep learning, enabling AI to handle vast datasets like images and speech.

Age of Artificial Intelligence (AI)



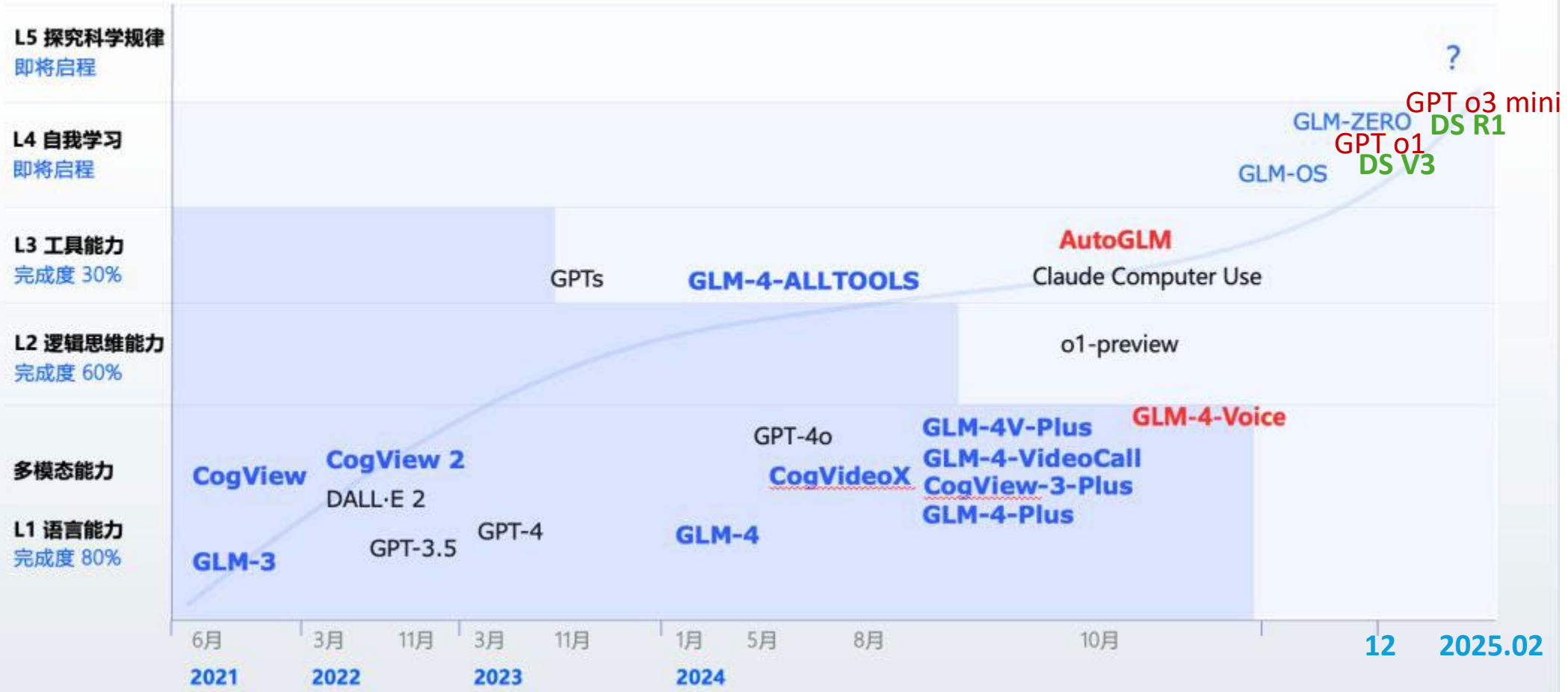
Brief History of LLM

图表1： 大模型发展时间线



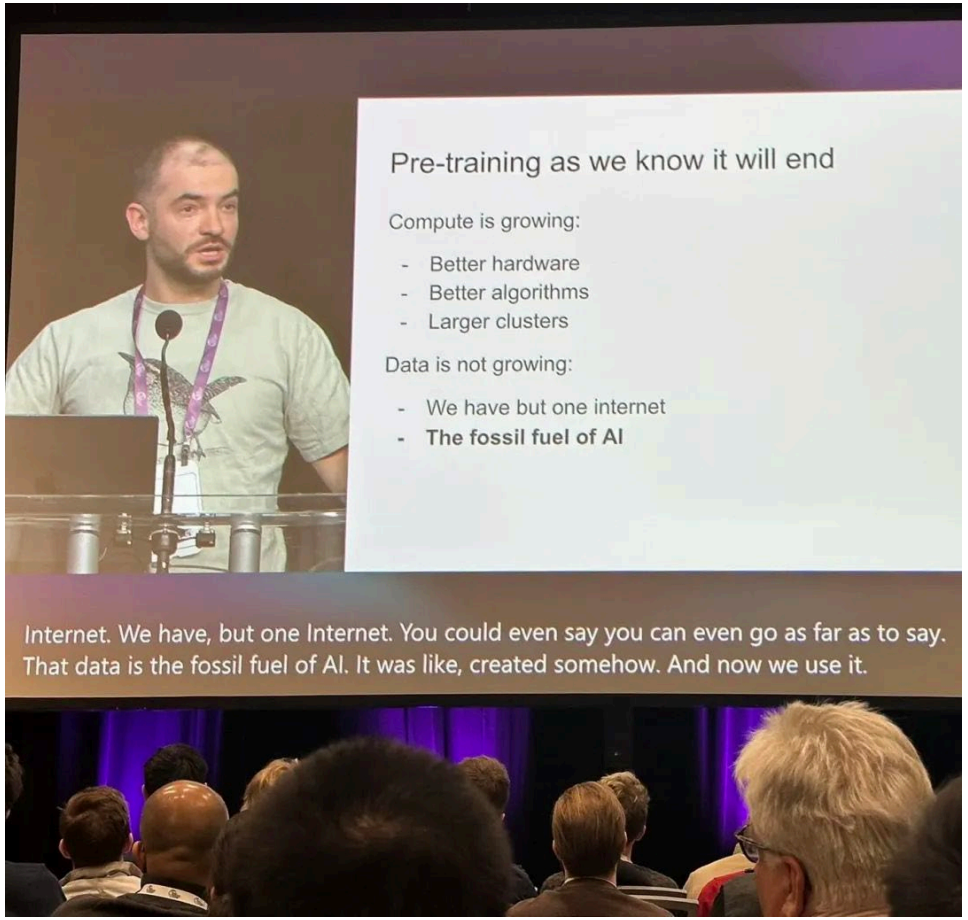
资料来源：A Survey of Large Language Models，中信建投

面向AGI的路线图



https://36kr.com/p/3102385679388422

https://36kr.com/p/3102385679388422



Ilya Sutskever at NeurIPS 2024 (Dec 2024)

Medical Data in the Age of AI

- **Types of Medical Data**:
  - **Electronic Health Records (EHRs)**: Patient data including medical history, diagnoses, and treatments.
  - **Medical Imaging**: X-rays, MRIs, CT scans, etc.
  - **Genomic Data**: DNA sequences and genetic information.
  - **Wearable Device Data**: Vital signs, activity data, etc.
- Role of Medical Data
  - **Training AI Models**: AI models require vast amounts of medical data to learn patterns and make accurate predictions.
  - **Data-Driven Insights**: Medical data allows AI to assist in diagnosing diseases, predicting outcomes, and personalizing treatment plans.
  - **Challenges**: Ensuring data quality, privacy, and compliance with regulations.

Biomedical Informatics ≈ Biomedical Data Science

Randolph A. Miller, MD, FACMI

- The **Cornelius Vanderbilt** Professor (Emeritus) of Biomedical Informatics.
- The **founding Chair** of the Department of Biomedical Informatics (DBMI) from **2001-2004**.
- The initial DBMI mission was to develop and evaluate leading-edge **biomedical software applications** to improve the **quality of care**, promote **research**, and enhance **patient safety**.

AI in Medicine

- AI in **Medical Diagnostics**
  - **AI for Image Recognition**: Using deep learning to analyze medical images like X-rays, MRIs, and CT scans for early disease detection (e.g., detecting cancer).
  - **AI in Pathology**: AI-powered systems to analyze pathology slides.

nature reviews clinical oncology

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › nature reviews clinical oncology › research highlights › article

Research Highlight | Published: 21 January 2020

BREAST CANCER

AI outperforms radiologists in mammographic screening

David Killock

Nature Reviews Clinical Oncology **17**, 134 (2020) | Cite this article

11k Accesses | **297** Altmetric | Metrics

AI in Medicine

- AI in **Personalized Medicine**
  - **Precision Medicine**: AI models can process genomic data to tailor treatments based on individual genetic makeup.
  - **Predictive Analytics**: AI algorithms can predict the likelihood of disease recurrence and suggest the most effective treatment options.

J Med Internet Res. 2018 Sep 25;20(9):e11087. doi: 10.2196/11087

Using Artificial Intelligence (Watson for Oncology) for Treatment Recommendations Amongst Chinese Patients with Lung Cancer: Feasibility Study

Chaoyuan Liu [1], Xianling Liu [1], Fang Wu [1], Mingxuan Xie [2], Yeqian Feng [1], Chunhong Hu [1,✉]

Editor: Carlos Luis Parra-Calderón

Reviewed by: Francisco Nuñez-Benjumea, Edward Meinert, Robert Robinson

Author information · Article notes · Copyright and License information

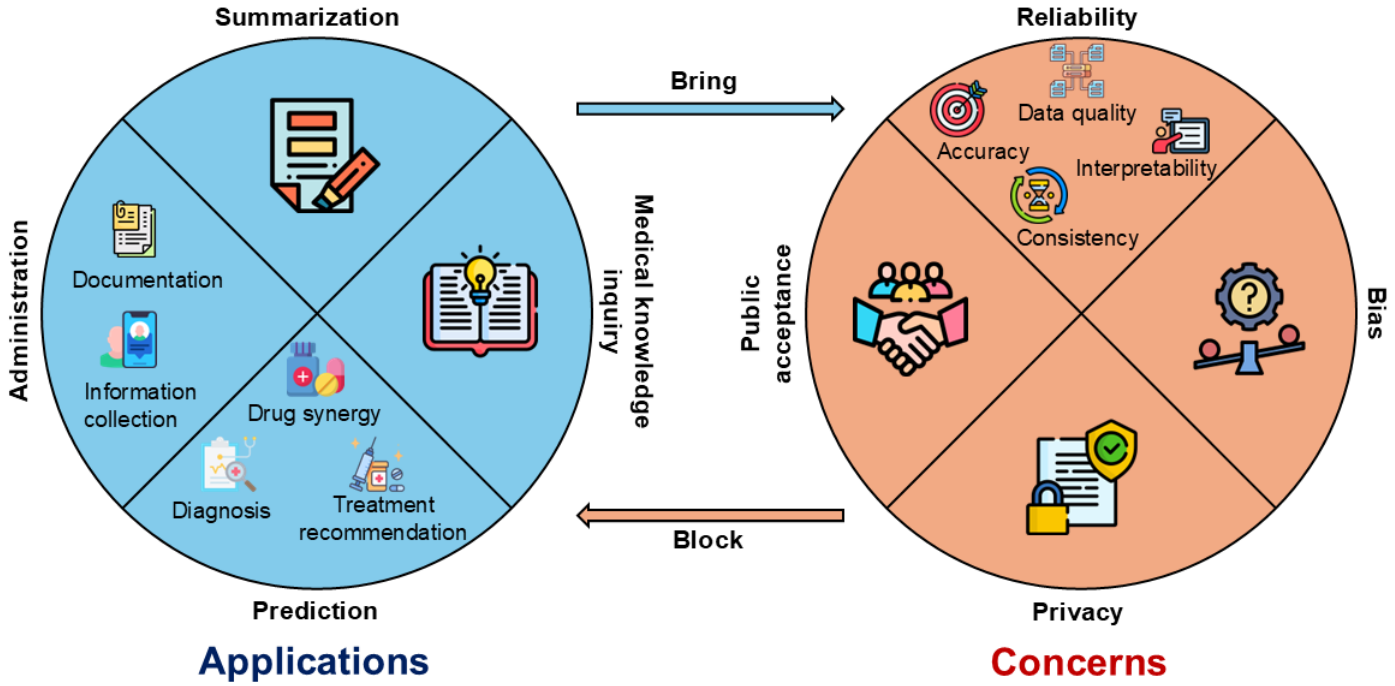
PMCID: PMC6231834 PMID: 30257820

AI in Medicine

- AI in **Drug Discovery and Development**
  - **Accelerating Drug Discovery**: AI analyzes massive datasets of molecular information to identify potential drug candidates.
  - **AI for Clinical Trials**: AI is used to identify suitable patient cohorts, predict trial outcomes, and optimize trial designs.

Applications and Concerns of Large Language Models in Health Care

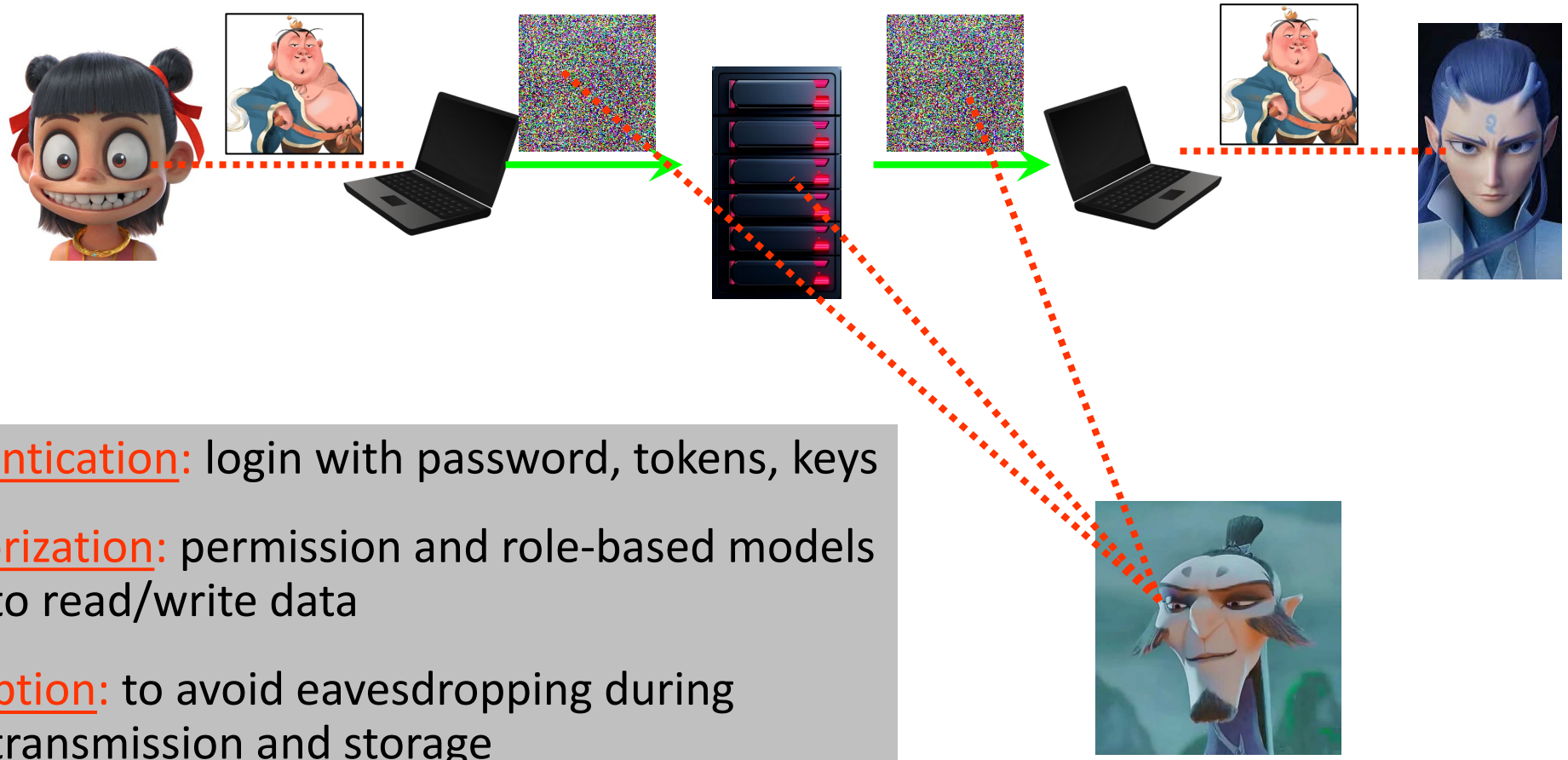
- A summary of the applications and concerns regarding LLMs in healthcare as communicated by 65 reviewed research papers selected from a pool of 820 articles sourced from PubMed, ACM, and IEEE, published before September 1st, 2023.



Wang L*, **Wan Z***, Ni C, Song Q, Li Y, Clayton E, Malin B, Yin Z. Applications and Concerns of ChatGPT and Other Conversational Large Language Models in Health Care: Systematic Review. *Journal of Medical Internet Research*. 2024 Nov 7;26:e22769.

So… What is Privacy?

Security for Privacy?



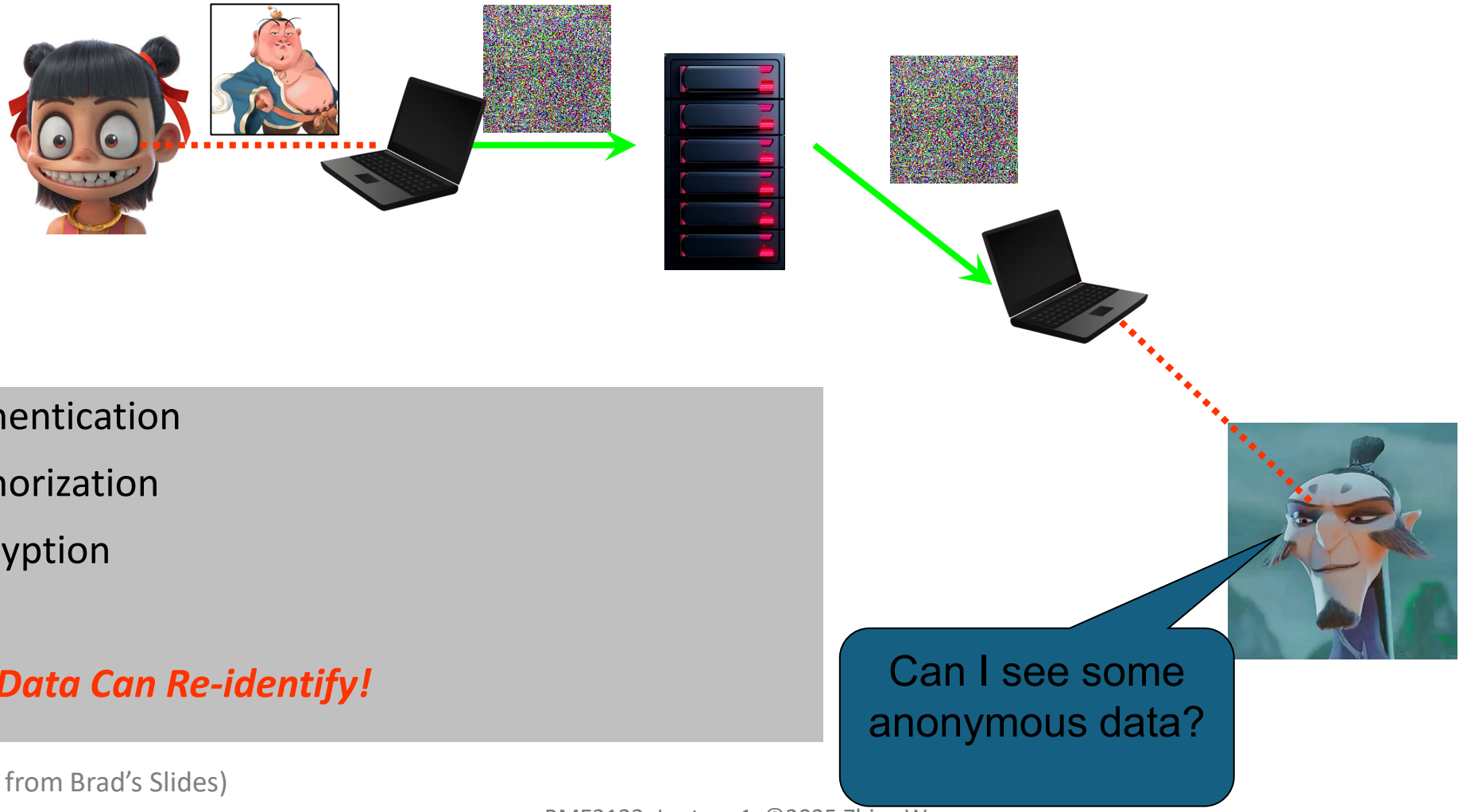
Authentication: login with password, tokens, keys

Authorization: permission and role-based models to read/write data

Encryption: to avoid eavesdropping during transmission and storage

(Adapted from Brad's Slides)

Security for Privacy?

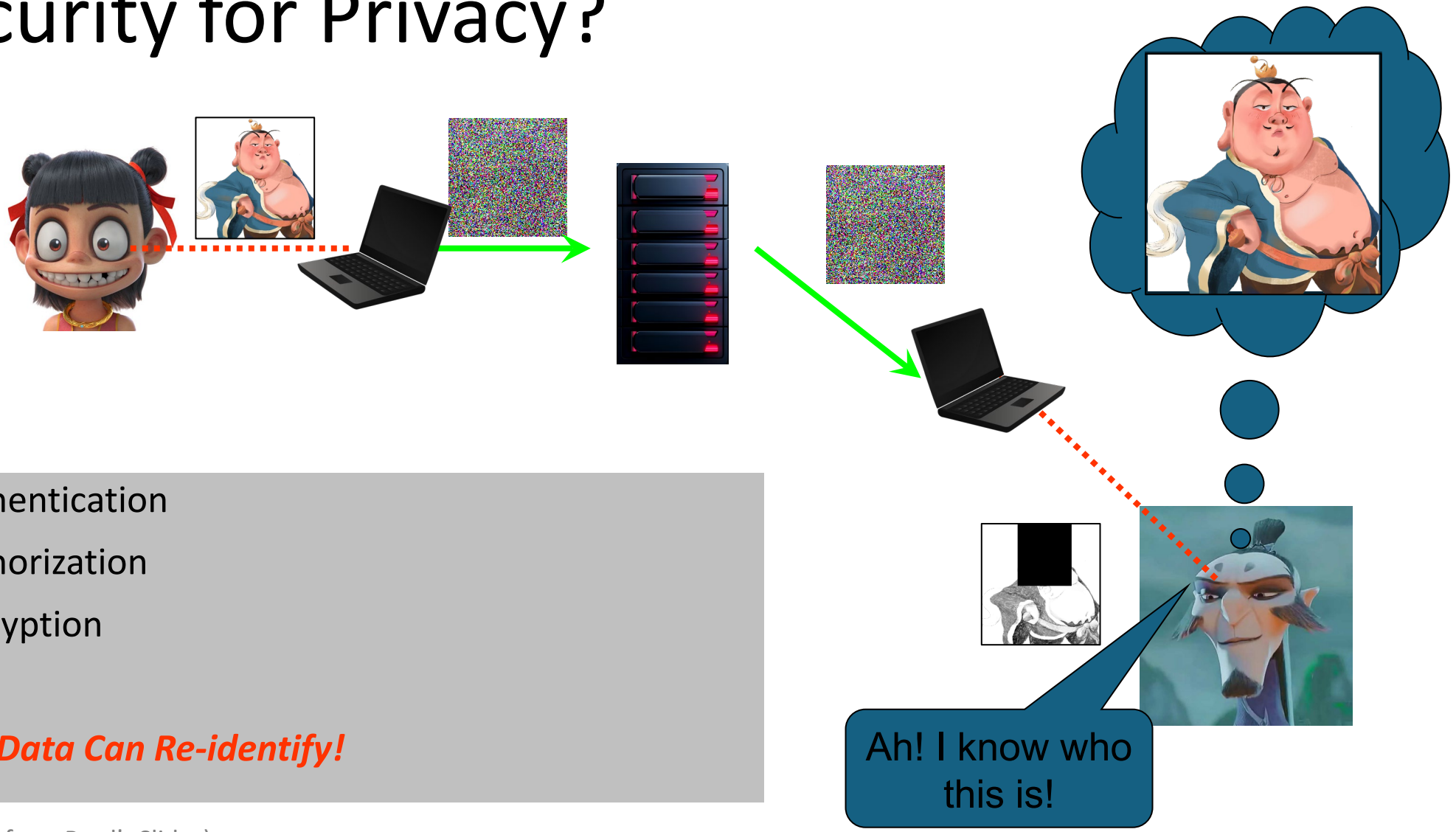


- Authentication
- Authorization
- Encryption

- ***But Data Can Re-identify!***

(Adapted from Brad's Slides)

Security for Privacy?



- Authentication
- Authorization
- Encryption

- ***But Data Can Re-identify!***

(Adapted from Brad's Slides)

Data Privacy Definitions

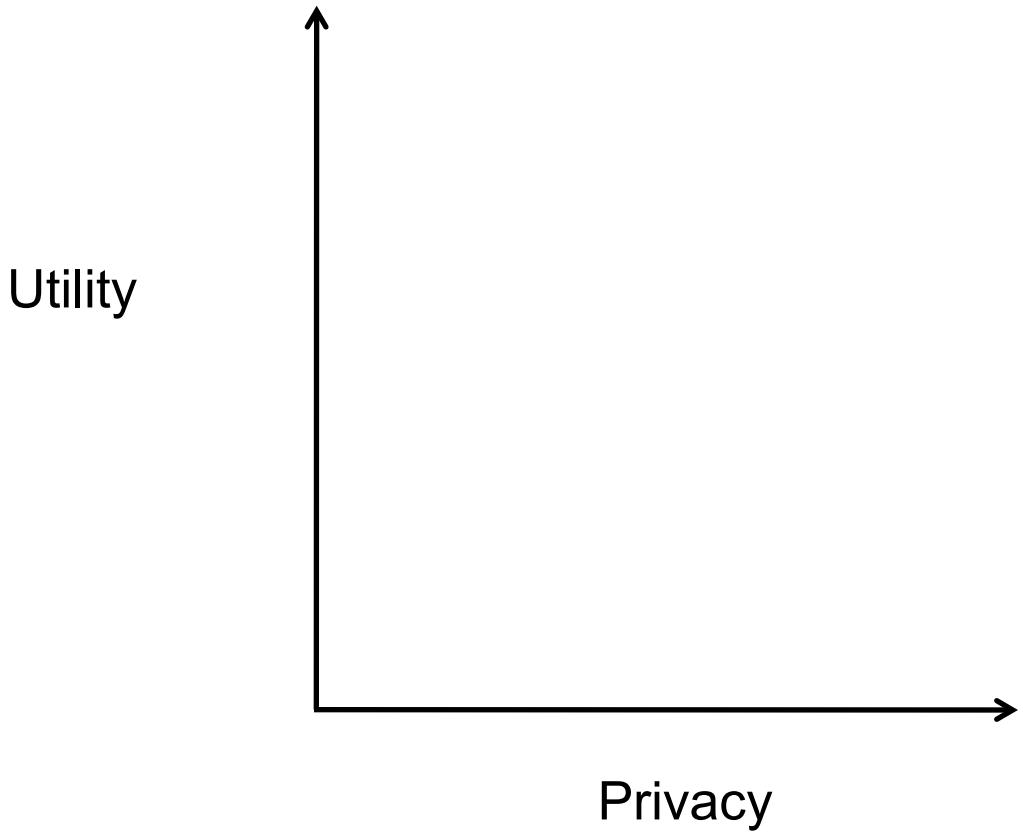
- **Data privacy** is the protection of personal information, ensuring that individuals have control over how their data is collected, used, and shared, while preventing unauthorized access and misuse. (ChatGPT-4o ←"define data privacy in one sentence")
- **Data privacy** is the protection and proper handling of personal information to ensure individuals' control over how their data is collected, used, shared, and stored, while safeguarding it from unauthorized access or misuse. (DeepSeek-R1 ←same prompt)
- The study of **computational solutions** for releasing data such that (paraphrase Sweeney)
- a) the data is practically useful (utility) while
- b) the aspects of the subjects of the data are not revealed (privacy).

Pioneer of Data Privacy

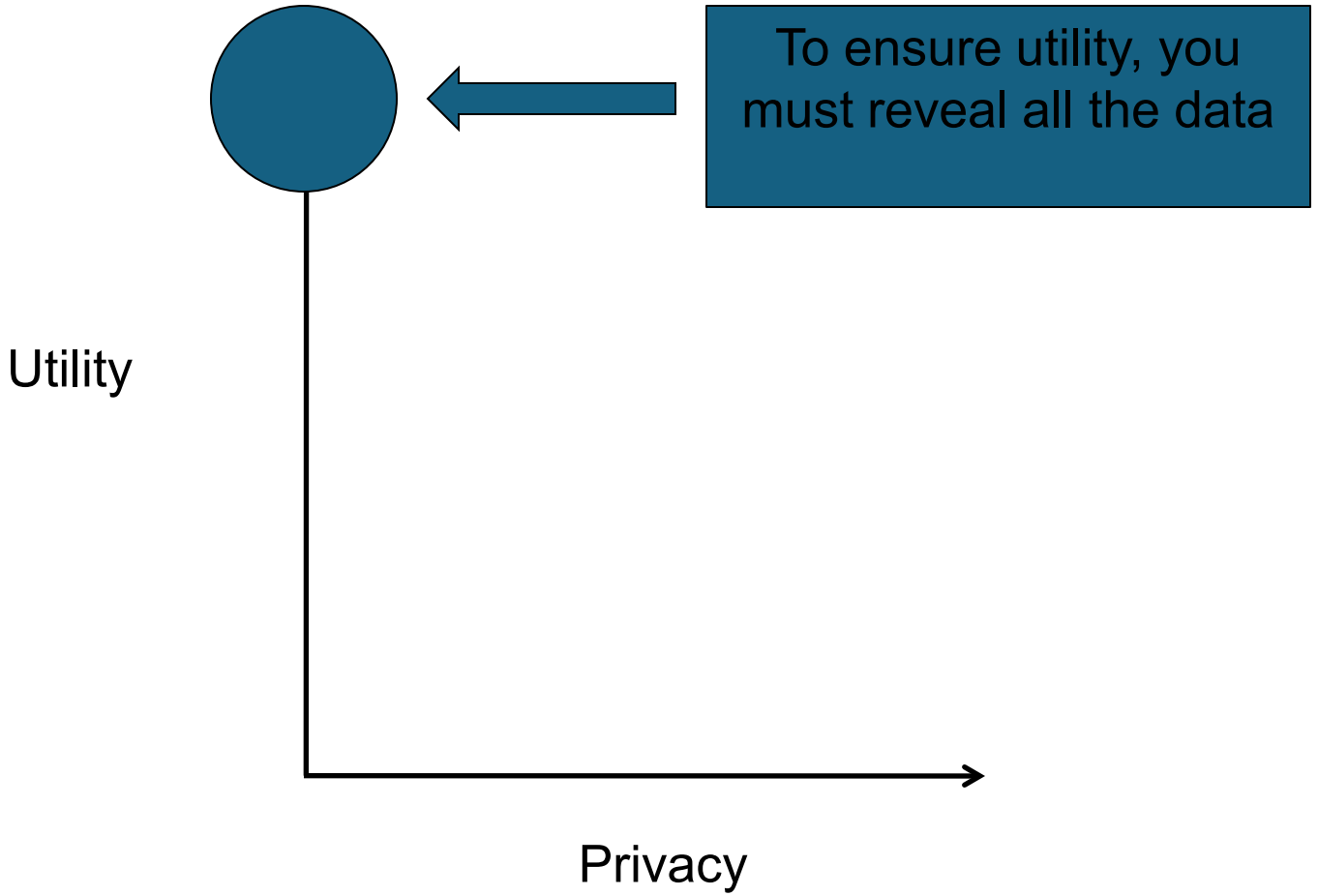
Latanya Sweeney, PhD, FACMI

- The Daniel Paul Professor of the Practice of Government and Technology at the Harvard University.
- In 2001, she founded the **Data Privacy Lab** at Carnegie Mellon University.
- She pioneered the field known as **data privacy**, launched the emerging area known as **algorithmic fairness.**
- Her best-known academic work is on the theory of ***k*-anonymity.**

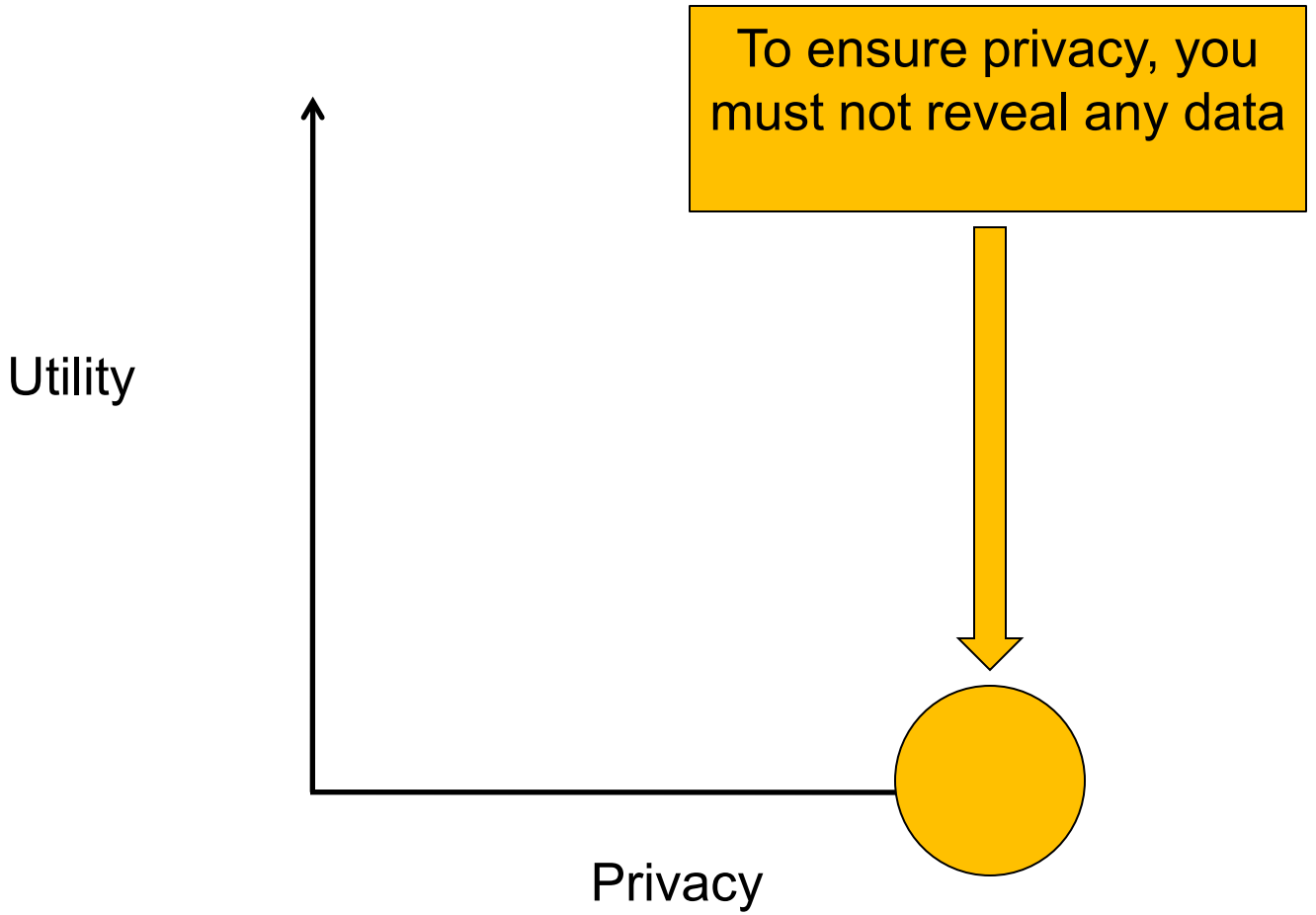
A Visual Perspective



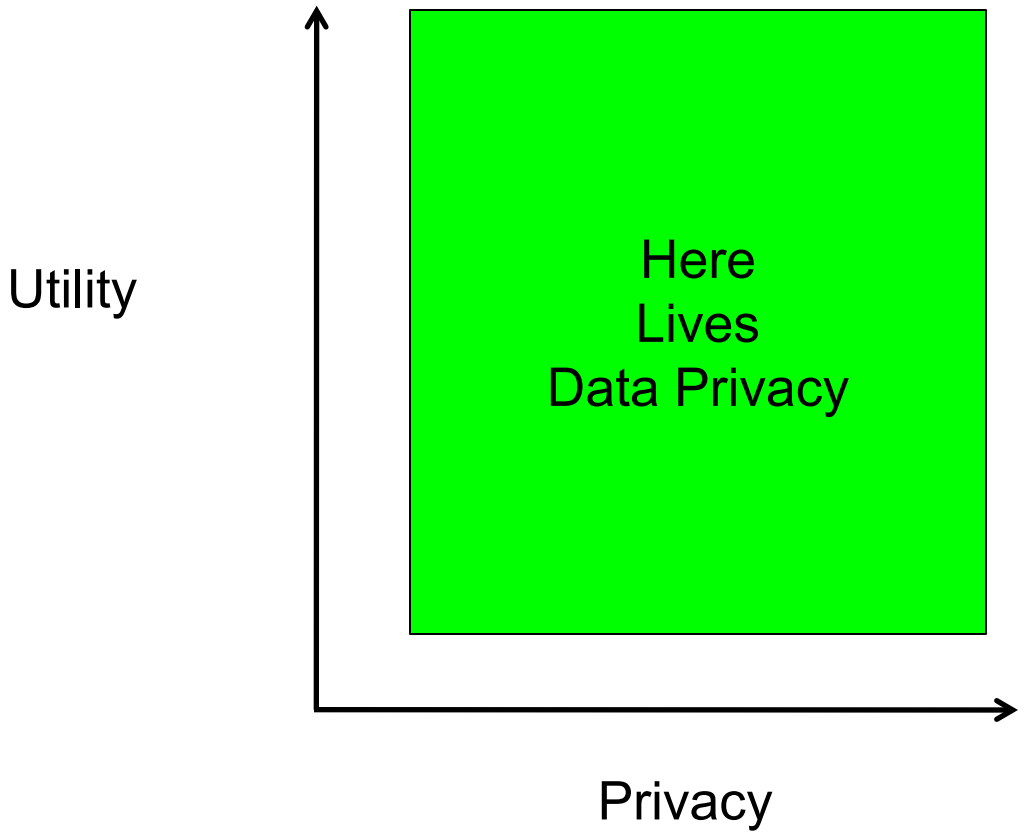
A Visual Perspective



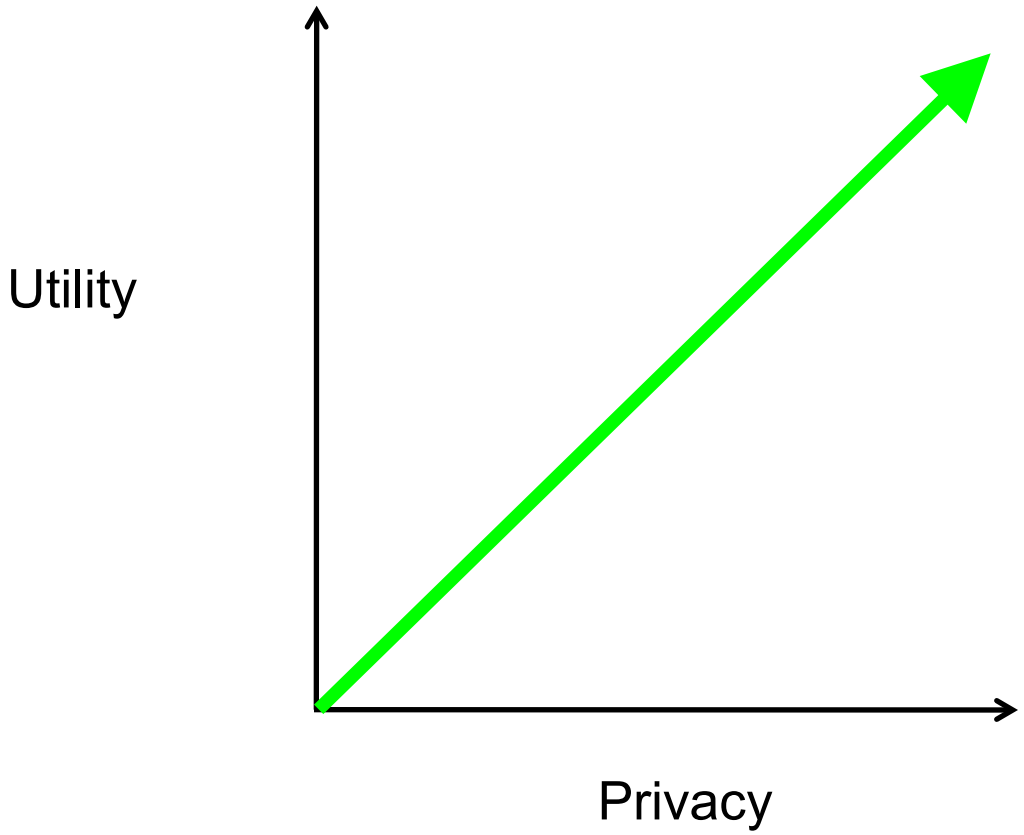
A Visual Perspective



A Visual Perspective

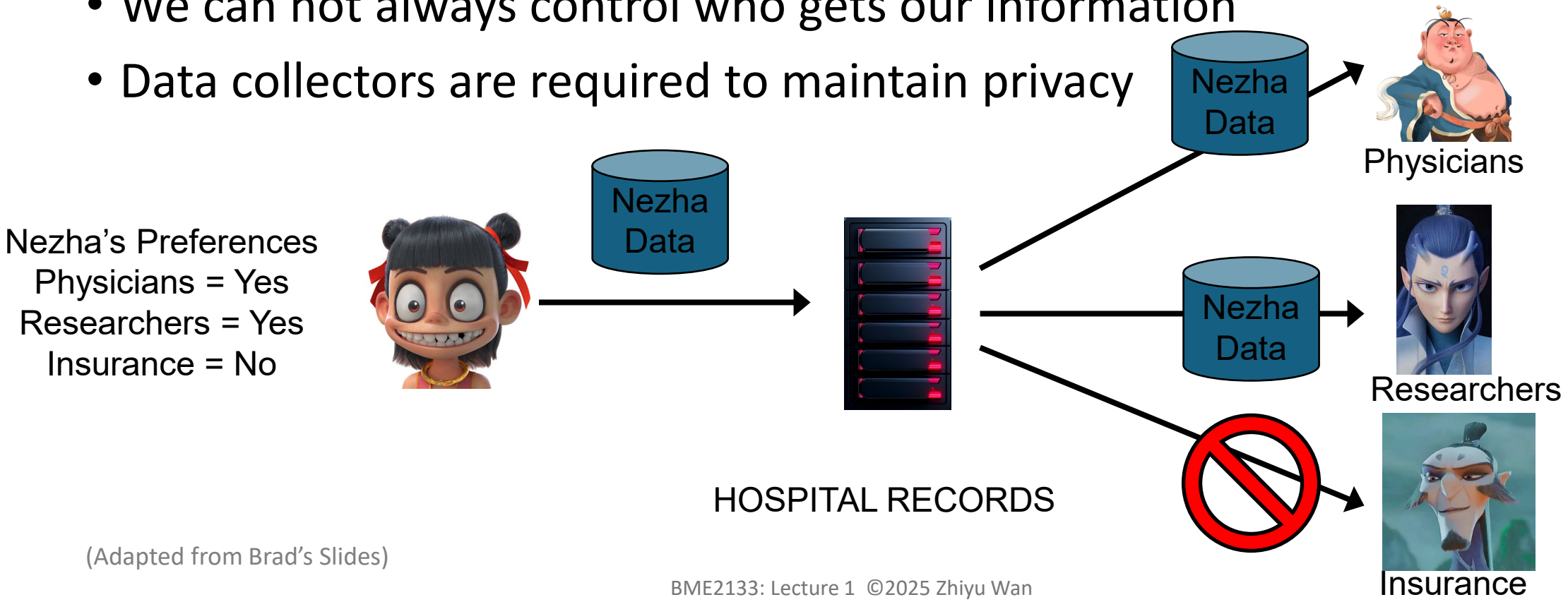


A Visual Perspective



Data sharing, Privacy, & Policy

- Individuals want control over who can – AND CAN NOT – view their health-related records
- We can not always control who gets our information
- Data collectors are required to maintain privacy



(Adapted from Brad's Slides)

Biomedical Information

- Not quite in the public
- But… information is shared for various purposes in various contexts
- How do you protect privacy of corresponding individuals?

(Adapted from Brad's Slides)

Readings for Next Lecture

- None.
- Optional
  - ❑《信息科学技术伦理与道德》Chs.8-10.
  - ❑《工程伦理》Ch.12.
  - ❑《信息科学技术伦理与道德》Chs.3&4.