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

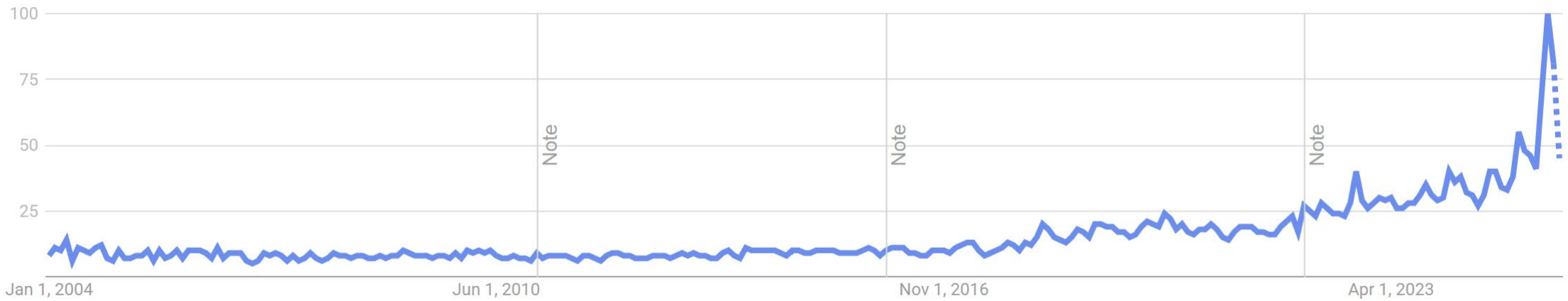
September 17, 2025

data privacy
Search term

+ Compare

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

Interest over time



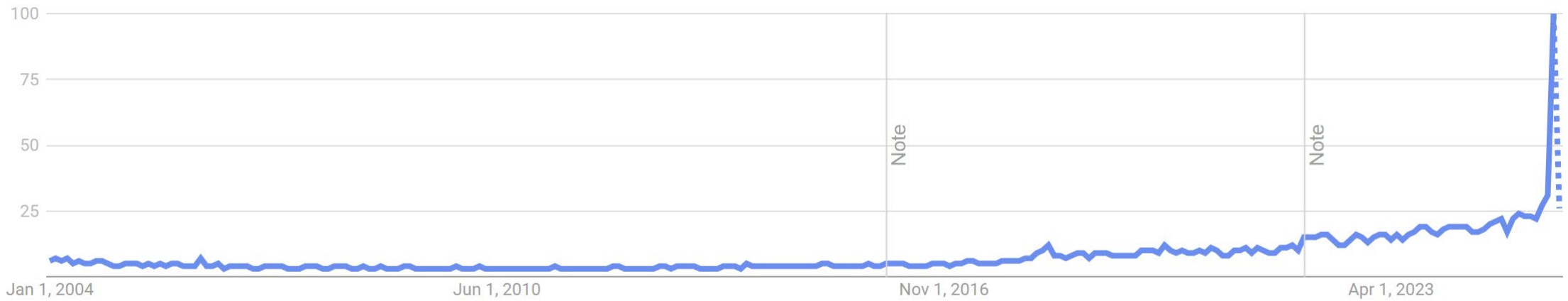
https://trends.google.com/trends/

data privacy
Search term

+ Compare

Worldwide | 2004 - present | All categories | Web Search

Interest over time

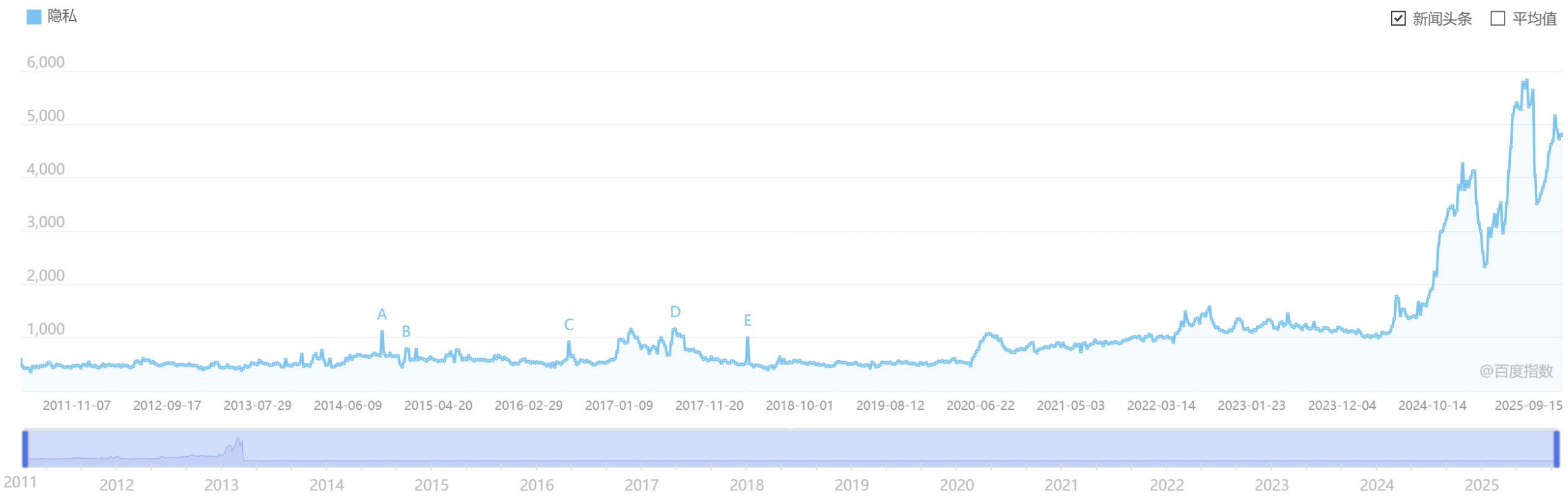


Worldwide

https://trends.google.com/trends/

关键词 | 隐私 | ＋添加对比 | 确定

搜索指数 | 对比时间段 | 2011-01-01 ~ 2025-09-15 | 全部 | PC+移动 | 全国



https://index.baidu.com/

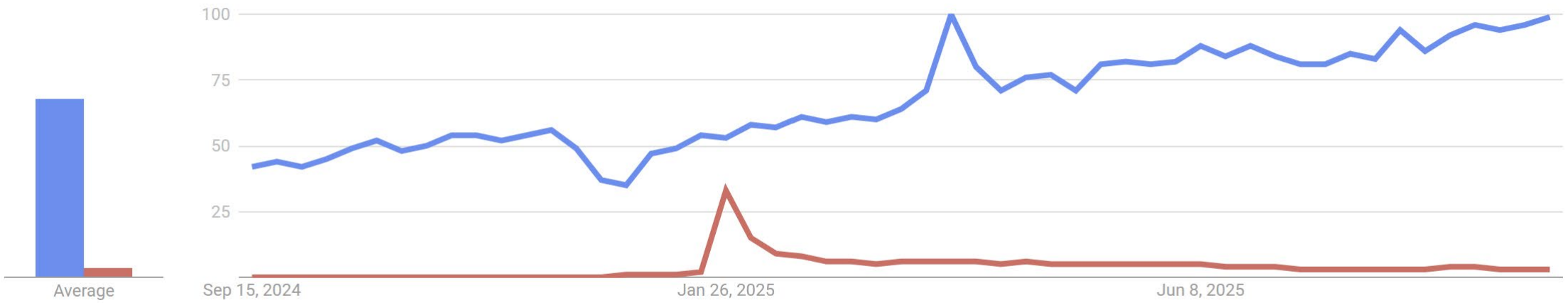
ChatGPT
Search term

DeepSeek
Search term

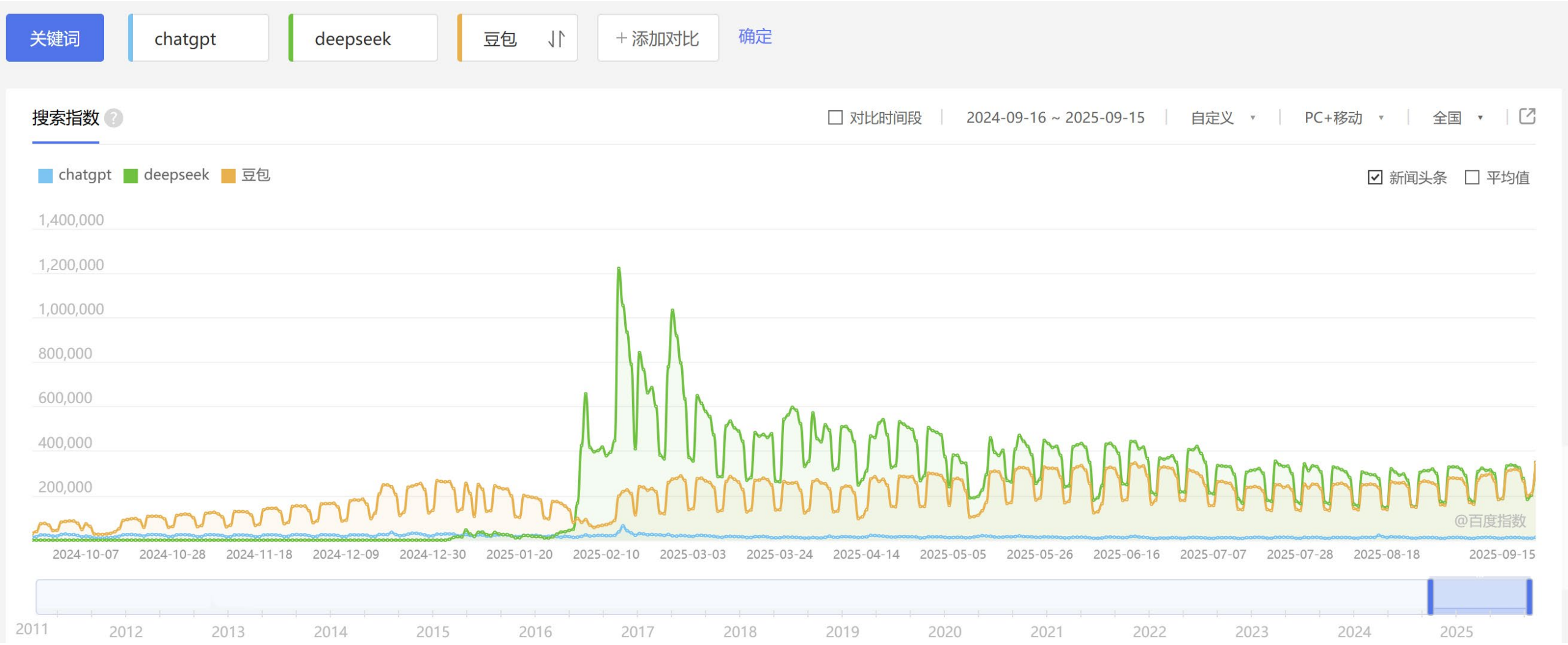
+ Add comparison

Worldwide | Past 12 months | All categories | Web Search

Interest over time



https://trends.google.com/trends/



https://index.baidu.com/

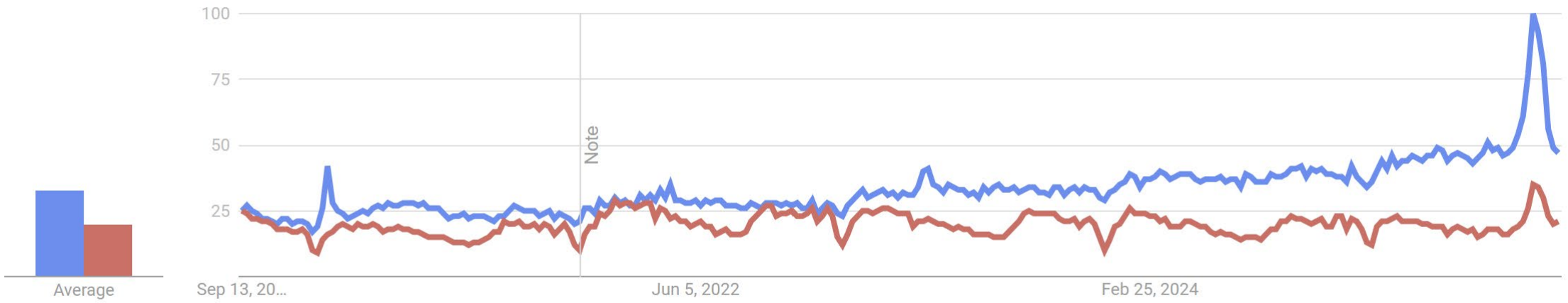
Privacy
Search term

Ethics
Search term

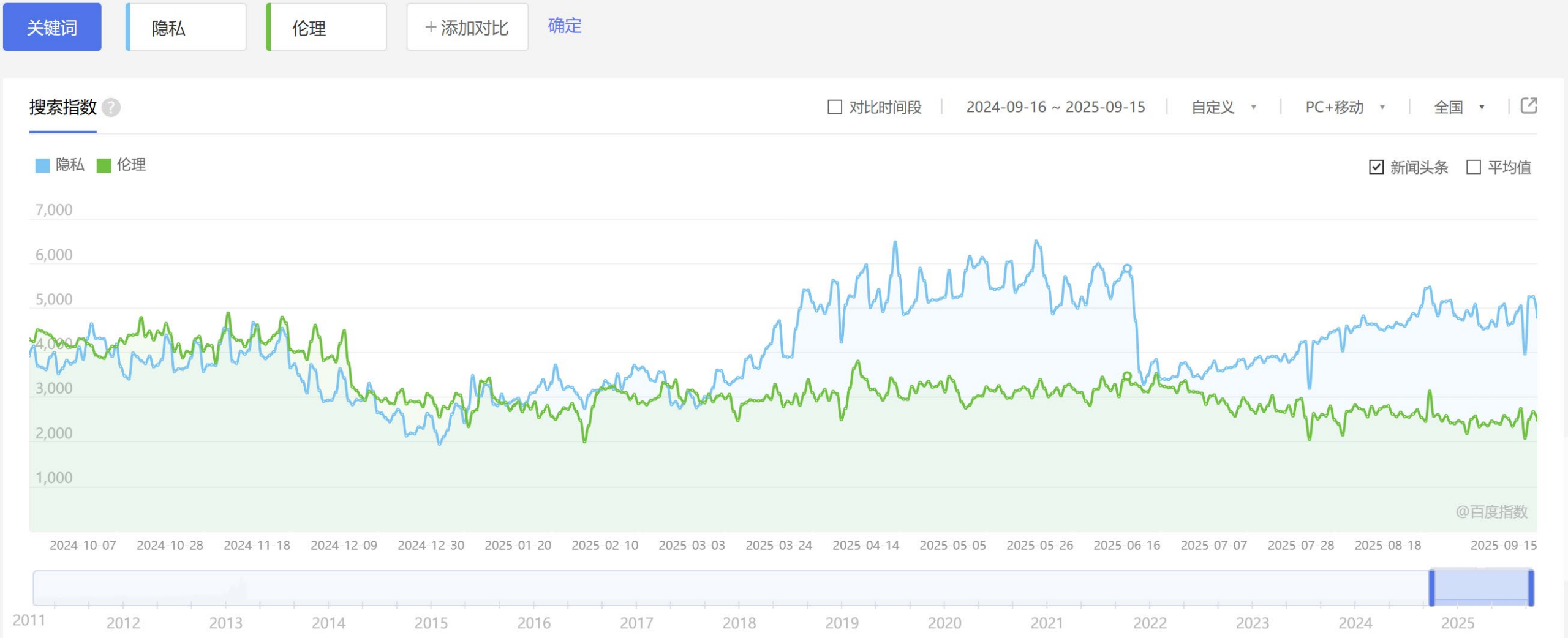
+ Add comparison

Worldwide | Past 5 years | All categories | Web Search

Interest over time



https://trends.google.com/trends/

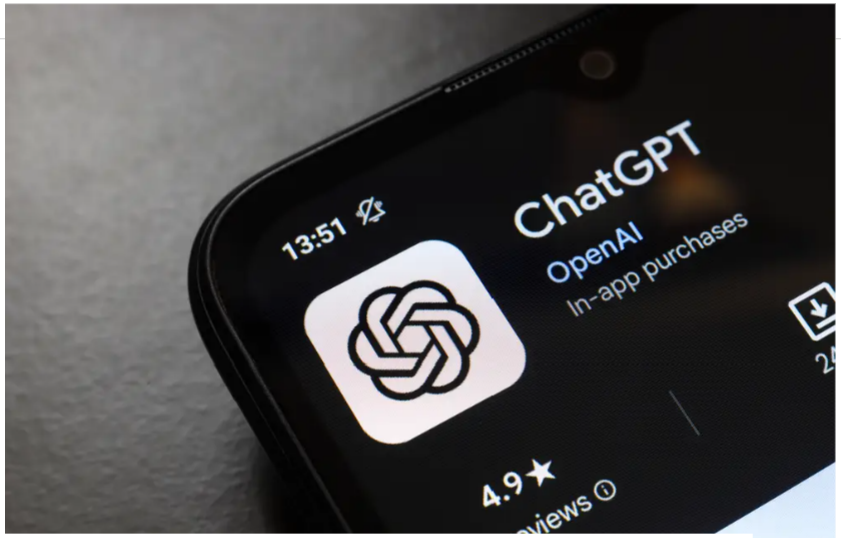

关键词
隐私
伦理
+ 添加对比
确定
搜索指数
对比时间段
2024-09-16 ~ 2025-09-15
自定义
PC+移动
全国
隐私
伦理
新闻头条
平均值
7,000
6,000
5,000
4,000
3,000
2,000
1,000
@百度指数
2024-10-07
2024-10-28
2024-11-18
2024-12-09
2024-12-30
2025-01-20
2025-02-10
2025-03-03
2025-03-24
2025-04-14
2025-05-05
2025-05-26
2025-06-16
2025-07-07
2025-07-28
2025-08-18
2025-09-15
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025

BUSINESS INSIDER

TECH

OpenAI quickly rolled back a new feature that users to make private conversations with Cha searchable

By Katherine Tangalakis-Lippert and Henry Chandonnet



OpenAI is removing a feature that lets users put ChatGPT activity on search engines over concerns that users could accidentally share private information. Jaque Silva/NurPhoto

Aug 1, 2025, 8:37 AM GMT+8 Share Save Add us on

- OpenAI is removing a feature that lets users put ChatGPT activity on search engines.
- The opt-in feature was a "short-lived experiment" that'll be gone by Friday, CISO Dane Stuckey said.
- The feature made it easier for users to accidentally share things they didn't mean to, Stuckey said.

OpenAI quickly rolled back a new feature that allowed users to make private conversations with ChatGPT "discoverable" after the launch was marred by concerns of accidental oversharing.

SMALL BUSINESS > ENTREPRENEURS

ChatGPT Warning: Change Your Business Data And Pr

By Jodie Cook, Senior Contributor. ⓘ Jodie Cook covers ChatGPT prompts & ...

Published Aug 08, 2025, 12:00pm EDT

Share Save Comment 0

Summary

Your ChatGPT chats are not private by default; sensitive busi for model training, risking your proprietary information. To p and competitive advantage, disable "Improve the model for settings. This crucial step keeps your private conversations a secure.

Show Less

ChatGPT warning: Change this setting to protect your business data and privacy
GETTY

Your ChatGPT chats are not private. Unless you toggle off a specific se everything you write into a ChatGPT chat can be used to train its mod

WIRED

NEWSLETTERS SUB

MATT BURGESS LILY HAY NEWMAN SECURITY JAN 27, 2025 5:18 PM

DeepSeek's Popular AI App Is Explicitly Sending US Data to China

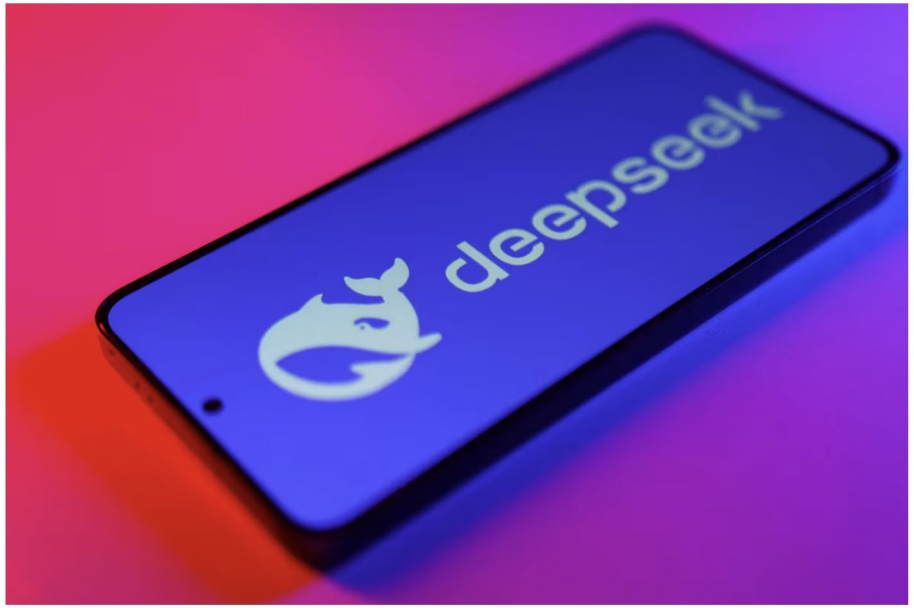
Amid ongoing fears over TikTok, Chinese generative AI platform DeepSeek says it's sending heaps of US user data straight to its home country, potentially setting the stage for greater scrutiny.

Reuters World Business Markets Sustainability Legal Commentary Technology Investigations More

DeepSeek faces ban from Apple, Google app stores in Germany

By Hakan Ersen and Miranda Murray

June 28, 2025 5:06 AM GMT+8 · Updated June 28, 2025



The Deepseek logo is seen in this illustration taken on January 29, 2025. REUTERS/Dado Ruvic/Illustration Purchase Licensing Rights

DeepSeek又被“拉黑”

新浪财经　2025-07-03 14:57　云南

近日，德国联邦数据保护专员迈克·坎普（Meike Kamp）正式向苹果（Apple）与谷歌（Google）提出请求，要求将中国人工智能初创企业深度求索的应用程序，从德国区App Store和Google Play下架。

韩国声称DeepSeek在未经用户同意情况下将用户数据传输到国外，外交部回应

环球时报　2025-04-24 16:36　北京

【环球时报-环球网报道 记者白云怡】在24日的外交部例行记者会上，有媒体提问称，韩国称，DeepSeek在未经用户同意的情况下，将用户数据和其他信息传输到国外。请问中方对此有何回应？

对此，中国外交部发言人郭嘉昆表示，我不了解你提到的具体情况。但是，我可以强调的是，中国政府高度重视并依法保护数据隐私和安全，从来没有、也不会要求企业或个人以违法形式采集或存储数据。中方一贯反对泛化国家安全的概念、将经贸科技问题政治化的做法，同时中方也将坚定维护中国企业的合法权益。

奥尔特曼曝ChatGPT对话尚未受法律保护：用户遇上诉讼时可能被公开

财联社　2025-07-25 22:38

财联社7月25日讯（编辑 赵昊）当下，越来越多的人将ChatGPT等聊天机器人用作心理咨询工具。但奥尔特曼警告道，这些对话可能不会像真正的心理医生那样受法律保护。

OpenAI被曝向搜索引擎公开ChatGPT共享对话，后因隐私风险叫停

IT之家　2025-08-01 15:27

Ai 导读

OpenAI关闭ChatGPT对话搜索引擎可见功能，因试验发现用户隐私泄露风险过高。此前公开分享的对话可能暴露求职简历等敏感信息，但需用户主动操作生成链接。谷歌强调索引权限始终由发布者掌控。

内容由AI智能生成　有用

IT之家 8 月 1 日消息，OpenAI 今日宣布，已从 ChatGPT 中**移除**允许用户将对话设为搜索引擎可见的功能。公司称，这项短期试验“让用户无意中泄露隐私的风险过高”。

据外媒 TechCrunch 今日报道，此前，如果在谷歌、必应等搜索引擎中限定搜索“https://chatgpt.com/share”域名，就能**找到他人公开分享的 ChatGPT 对话**。

7亿人每周狂发180亿条消息！OpenAI首次揭秘ChatGPT最火用途

新智元 2025-09-16 14:27

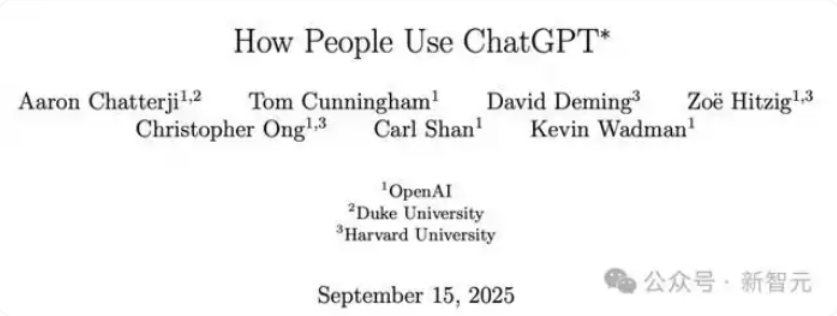
AI导读

ChatGPT周活用户超7亿，70%对话用于生活场景：写作、查询、实用建议成主流，女性用户激增52%；Claude则主攻代码编写，39%用户直接交付完整任务，开发者调试时间锐减。两大AI工具重塑工作与生活，技术红利正加速渗透全球。

内容由AI智能生成 有用 |

ChatGPT首份使用报告出炉了！

今天，OpenAI联手杜克、哈佛一共发布了「人们如何使用ChatGPT」，全文共63页。



How People Use ChatGPT*

Aaron Chatterji[1,2] Tom Cunningham[1] David Deming[3] Zoë Hitzig[1,3]
Christopher Ong[1,3] Carl Shan[1] Kevin Wadman[1]

[1]OpenAI
[2]Duke University
[3]Harvard University

September 15, 2025

报告地址：https://cdn.openai.com/pdf/a253471f-8260-40c6-a2cc-aa93fe9f142e/economic-research-chatgpt-usage-paper.pdf

自2022年11月上线到2025年7月，报告覆盖了近三年的海量数据，重点剖析了ChatGPT的使用情况。

截至7月，**ChatGPT周活跃用户已超7亿**，约占全球成年总人口10%，每周消息总量高达180亿。

· 哪些人在使用ChatGPT?

· 人们用ChatGPT都在做什么?

OpenAI研究采用了更科学的方法，即基于内部对话数据，并使用自动化分类结合隐私保护技术展开分析。

September 15, 2025 Research Publication Global Affairs

How people are using ChatGPT

Largest study to date of consumer ChatGPT usage shows demographic gaps shrinking, economic value being created through both personal and professional use.

150万次对话，覆盖了三大数据集。具体包括：

- **Growth数据：**2022年11月-2025年9月，所有付费用户每日消息总量，以及基础人口统计信息
- **分类消息数据：**2024年5月-2025年6月，随机抽取约100万条去标识化信息，经过粗粒度分类
- **就业数据：**约13万用户公开的职业与教育信息聚合生成

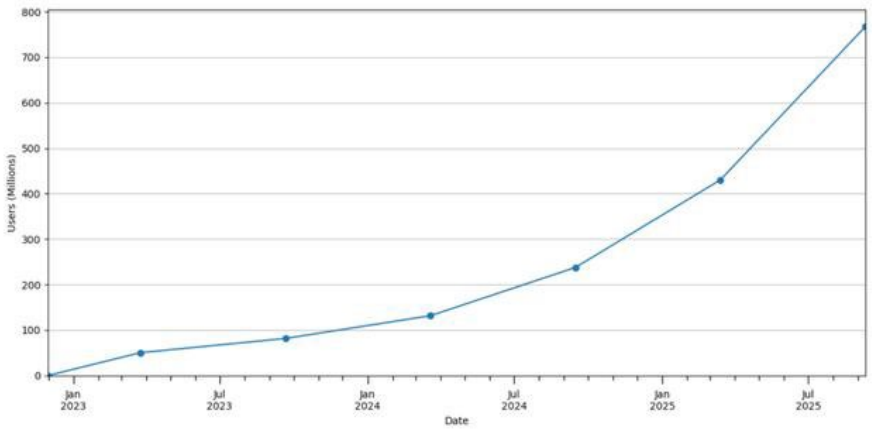


Figure 3: Weekly active ChatGPT users on consumer plans (Free, Plus, Pro), shown as point-in-time snapshots every six months, November 2022–September 2025.

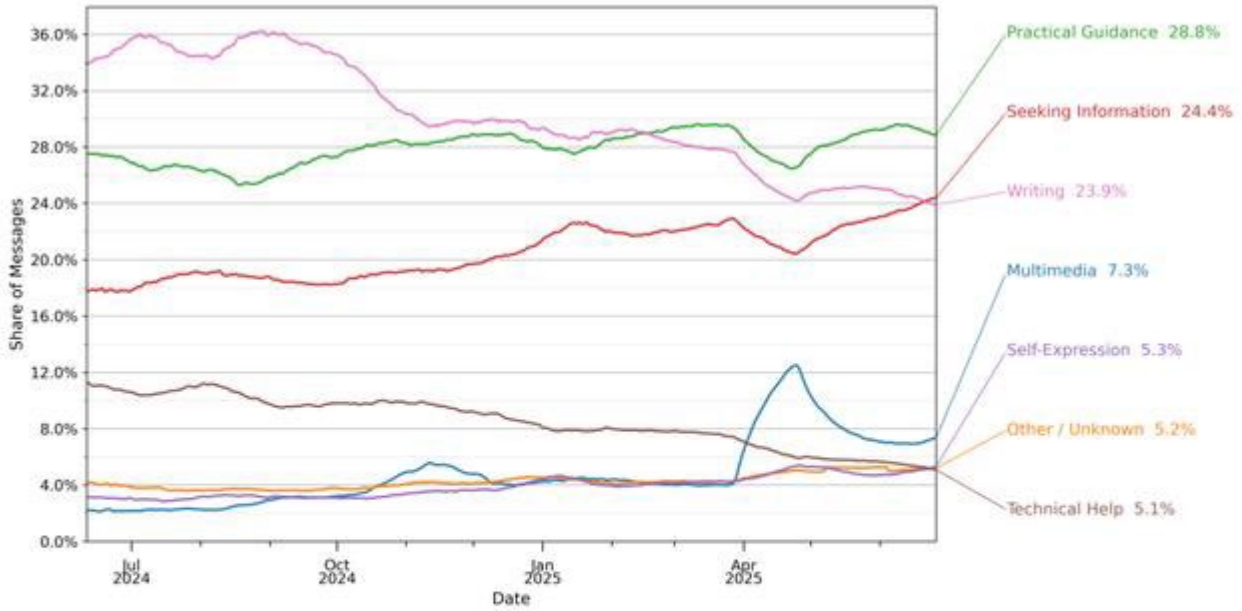


Figure 7: Share of consumer ChatGPT messages broken down by high level conversation topic, according to the mapping in Table 3. Values are averaged over a 28 day lagging window. Shares are calculated from a sample of approximately 1.1 million sampled conversations from May 15, 2024 through June 26, 2025. Observations are reweighted to reflect total message volumes on a given day. Sampling details available in Section 3.

Topic	Conversation Category
Writing	Edit or Critique Provided Text
	Personal Writing or Communication
	Translation
	Argument or Summary Generation
	Write Fiction
Practical Guidance	How-To Advice
	Tutoring or Teaching
	Creative Ideation
	Health, Fitness, Beauty, or Self-Care
Technical Help	Mathematical Calculation
	Data Analysis
	Computer Programming
Multimedia	Create an Image
	Analyze an Image
	Generate or Retrieve Other Media
Seeking Information	Specific Info
	Purchasable Products
	Cooking and Recipes
Self-Expression	Greetings and Chitchat
	Relationships and Personal Reflection
	Games and Role Play
Other/Unknown	Asking About the Model
	Other
	Unclear

Table 3: Coarse Conversation Topics and Underlying Classifier Categories

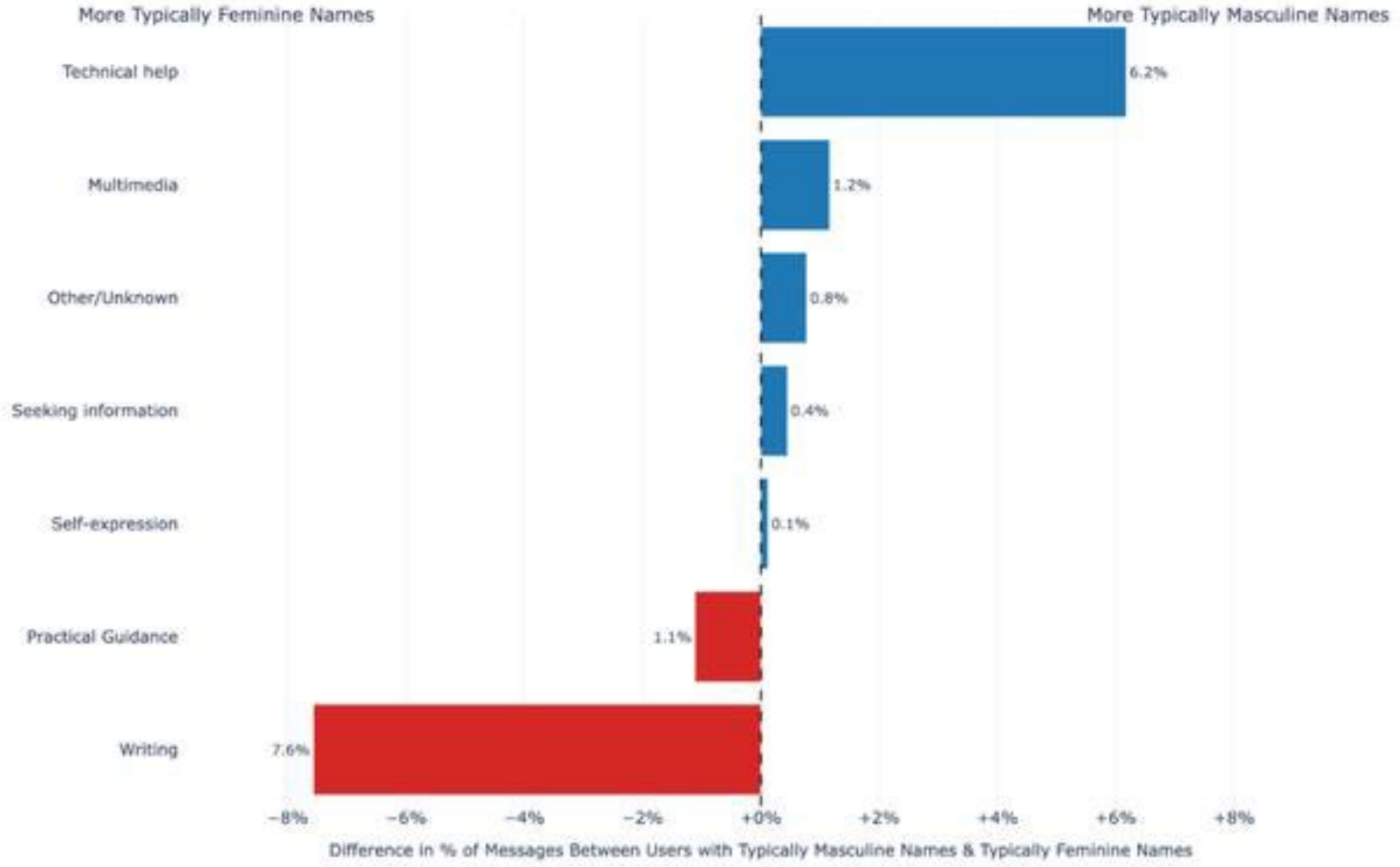


Figure 19: Difference in share of topic prevalence in messages by users with typically masculine/feminine first name. We draw on a uniform sample of 1.1M ChatGPT accounts, subject to the same user exclusion principles as other datasets we analyze. Note that this is a separate sample than those described in Section 3. First names are classified as typically masculine or typically feminine using public aggregated datasets of name-gender associations. Topics are aggregated groupings from a classifier whose prompt we provide in Appendix A.

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.

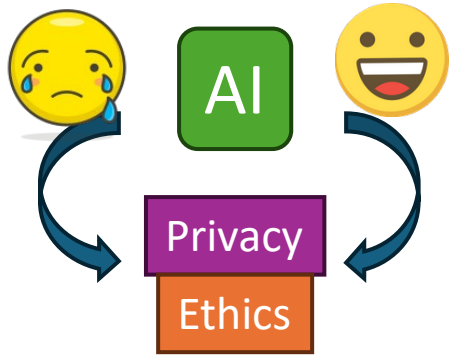
Led by UC Berkeley engineer Anil Aswani, the study suggests current laws and regulations are nowhere near sufficient to keep an individual's health status private in the face of AI development. The research was published Dec. 21 in the *JAMA Network Open* journal.

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 & Fridays (Odd Week), 15:00-15:45, 15:55-16:40
- Where: SLST, A103

- Office Hours: Upon Request
- Teaching Assistant:
  - Sihan Xie (xiesh2024@shanghaitech.edu.cn)
  - Hongzhu Jiang (jianghzh2024@shanghaitech.edu.cn)
- Instructor: Zhiyu Wan (wanzhy@shanghaitech.edu.cn)

Goals of this lecture

- Know more about this course
  - Instructor
  - Objectives
  - Grading policies
  - 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/)
- Research Areas
  - Biomedical Data Privacy
  - AI in Medicine
  - Synthetic Data Generation
  - Responsible AI
  - AI Ethics
  - …

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: Sihan Xie, Hongzhu Jiang
Semester: Fall 2025
Time: Wednesdays & Fridays (Odd Week) , 15:00-15:45, 15:55-16:40
Location: School of Life Science and Technology Room A103
Office Hours: Upon request, Location: BME Building, Room 228

Course Syllabus (PDF)

First Day of Class: September 17, 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 solid foundation 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 data privacy and ethics in the age of artificial intelligence; the second part discusses social and legal approaches to protecting data privacy and ethics; the third part covers technical methods for privacy and ethics protection; and the fourth part applies these privacy and ethics protection methods to specific cases.

Schedule

(Note: This schedule is tentative and subject to change.)

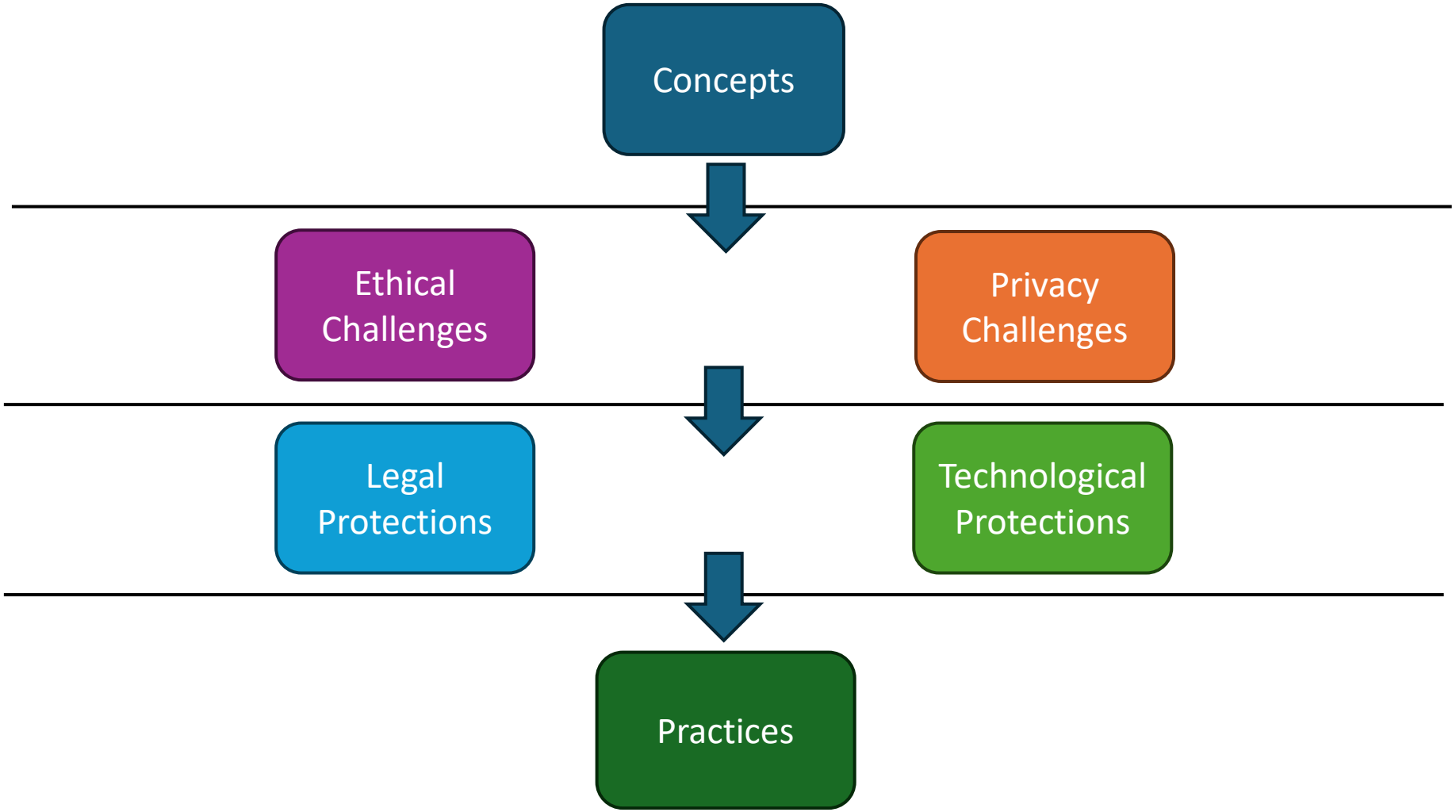
Week	Chapter	Teaching Contents	Reading	Assignments
Week 1, Wednesday Sept 17, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (a)	Course introduction. The role of medical data in the age of AI. Concept of data privacy and its importance.	/	/
Week 1, Friday Sept 19, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (b)	Concept of ethics and morality and their importance. 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.)	/
Week 2, Wednesday Sept 24, 15:00-16:40	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. Information security and privacy issues: personal data breaches, surveillance		

More to come (projects, homeworks, etc.) – links will be available from this schedule page

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

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

- 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, guest lectures.
- 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 Policies

- 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	40%
Homework Assignments	30% (+2.5%)
Reading Summaries	10% (+5%)
In-class quizzes	15% (+2%)
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 need to disclose and document the version number.

Reading Summaries

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

- There is no required textbooks for this course.
- Assigned readings will be available one 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 the instructors and 2 TAs 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 later in the semester)
- Do not be afraid to discuss your project ideas with the instructor!

Schedule

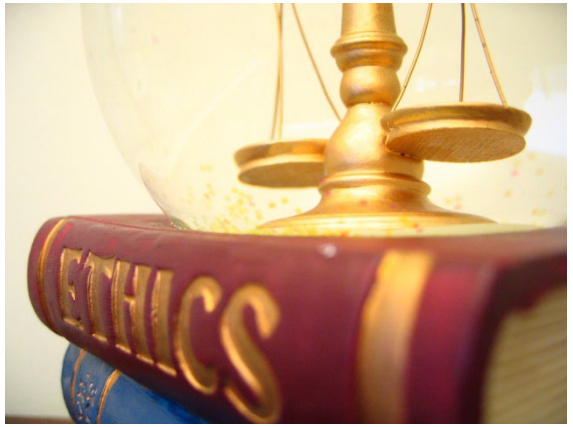
- Let’s look at the syllabus.

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

Ethics (Sept 19, 24, Oct 11, 15, 17, 22)

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

Quiz 1



Quiz 2

(Picture from Brad's Slides)

The Law and Regulations (Oct 29, 31)

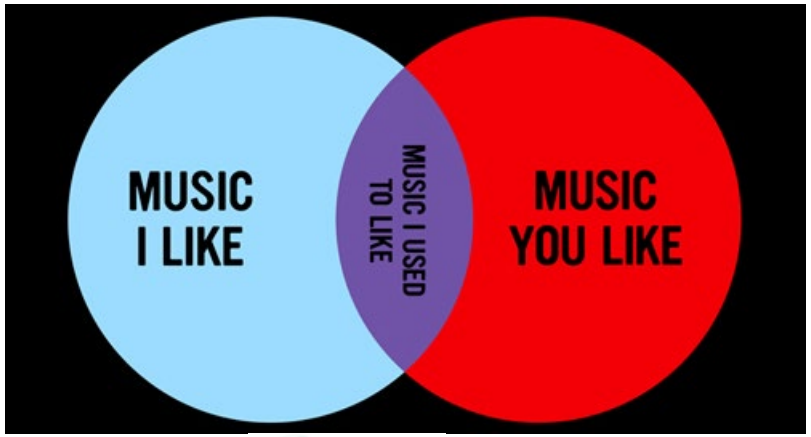
- The impact of international laws and regulations like HIPAA and GDPR on the impact of biomedical data.
- China’s data security law and personal information protection law.
- Compliance requirements for medical data sharing.

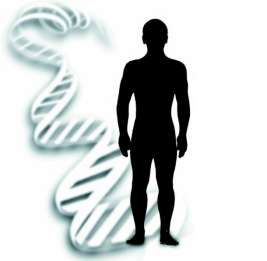
Quiz 3

(Picture from Brad’s Slides)

Privacy Risks of Biomedical Data (Nov 5, 12, 19, 26)

- 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



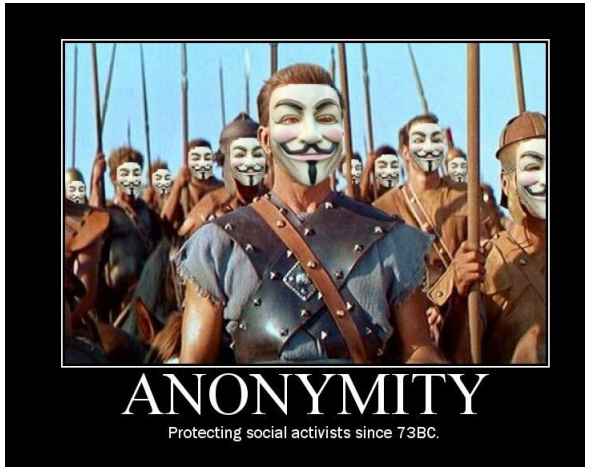


HW 1

(Pictures from Brad's Slides)

Common Privacy Protection Techniques for Medical Data (Nov 14, 28, Dec 3)

- Data de-identification techniques
  - K-anonymization
- Game-theoretic models
- Differential privacy
- Access control and audit techniques



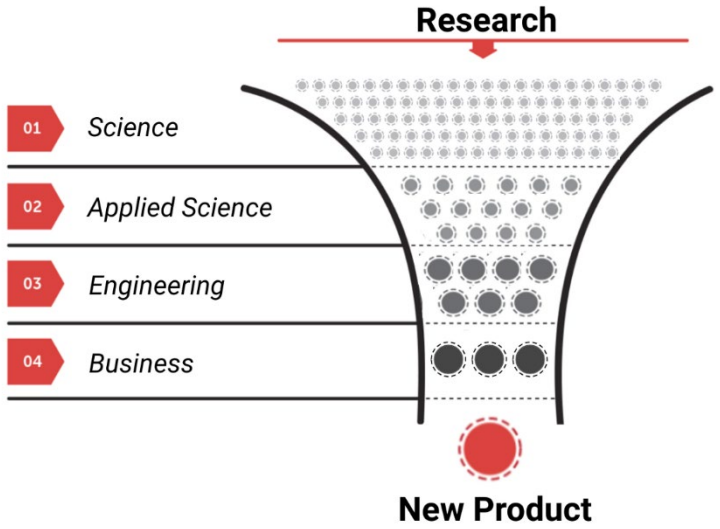
HW 2a

(Pictures from Brad's Slides)

Advanced Privacy Protection Techniques for Medical Data (Dec 10, 12, 17)

- Cryptographical methods
  - homomorphic encryption
  - secure multi-party computation
  - Encrypted hardware
- Federated learning
- Synthetic data generation
- Blockchain

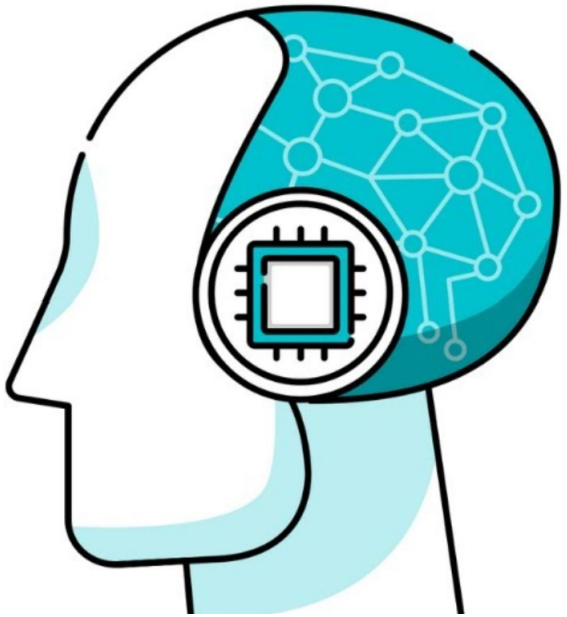
HW 2b



(Picture from Brad's Slides)

Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare (Dec 24, 26)

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



Project

Course Project Presentation (Dec 26, 31)

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

(Picture from Brad's Slides)

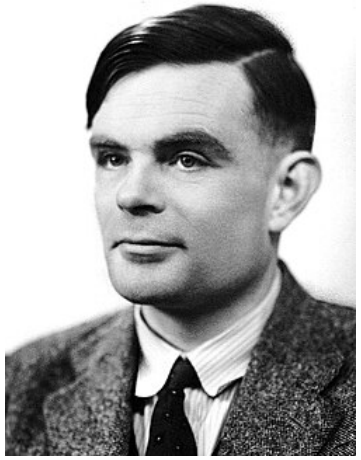
Introduction to AI

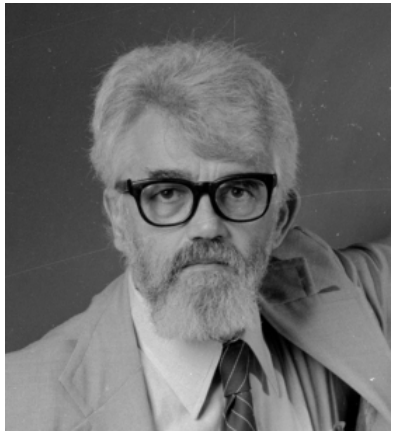
- **Definition of AI**: AI refers to the simulation of human intelligence in machines that are programmed to think, learn, and make decisions.

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

Development of AI

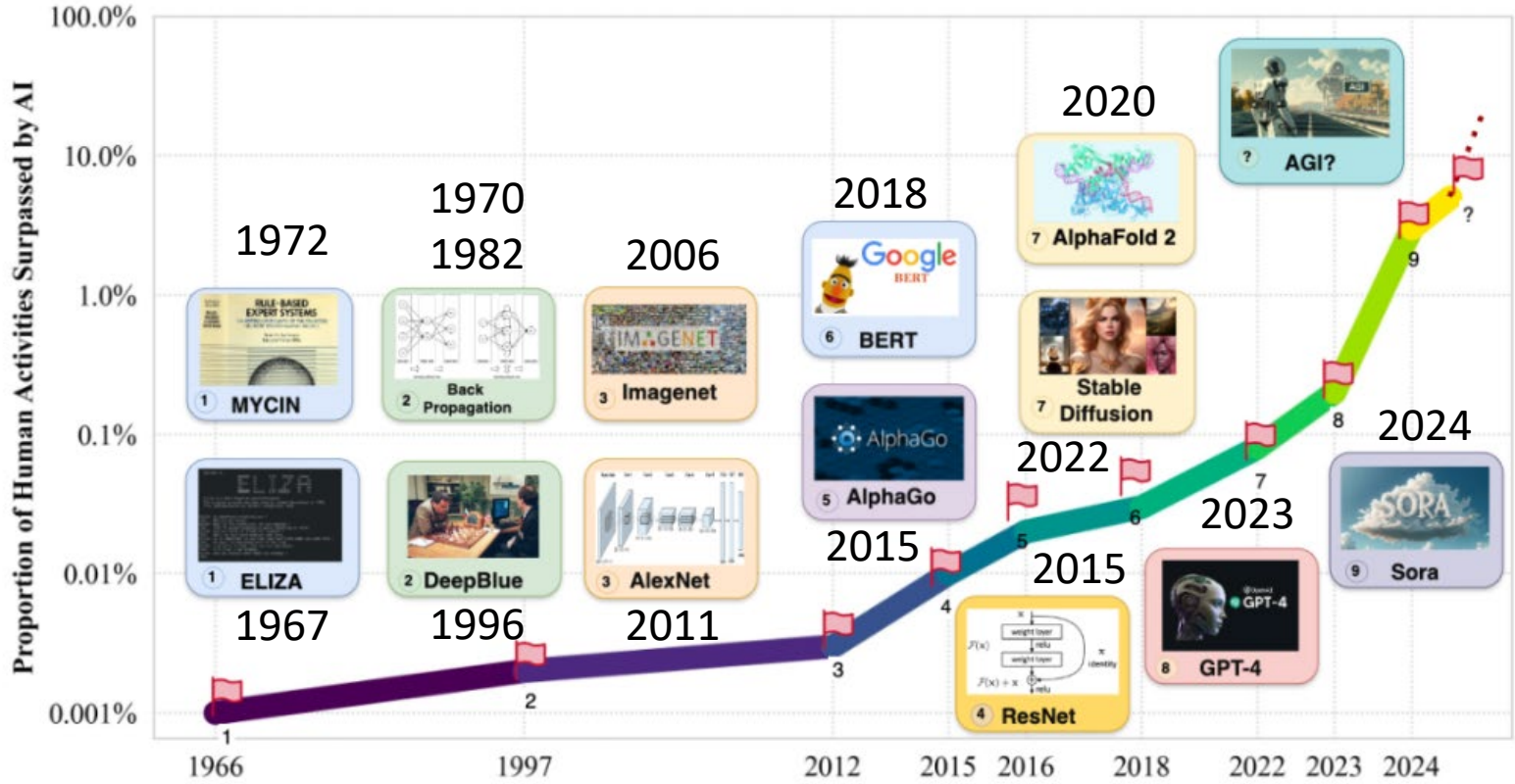
- **Early Development**: The origins of AI date back to the 1950s, with pioneers like Alan Turing and John McCarthy.

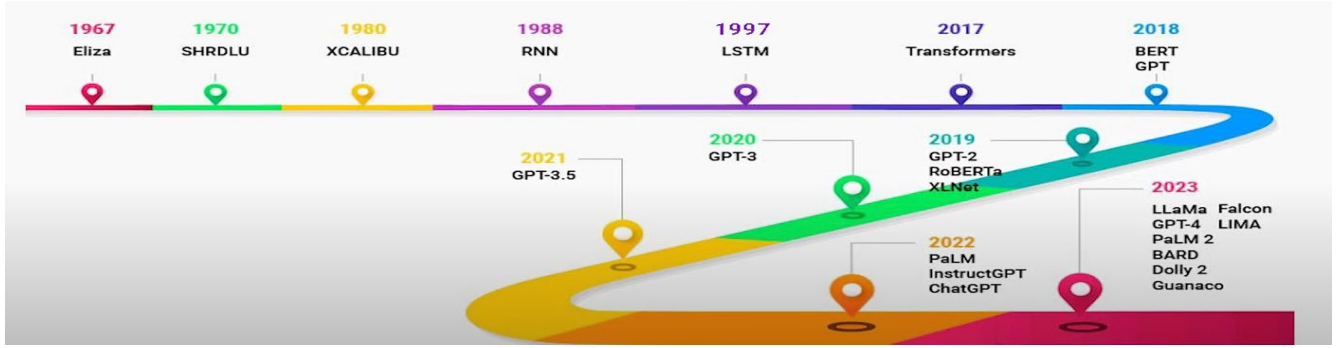




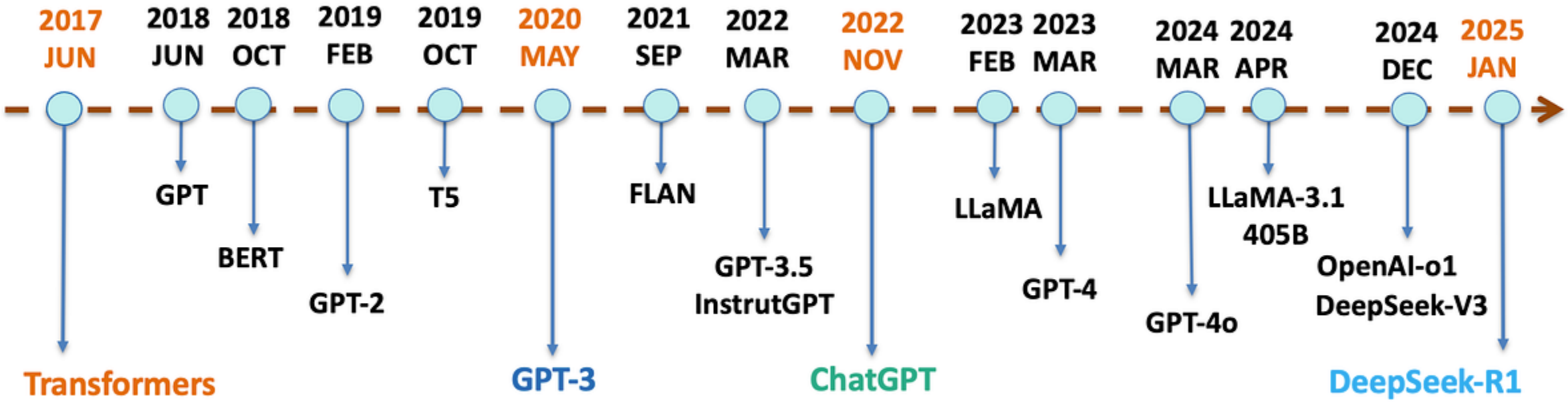
- **Advancements in Machine Learning**:
  - 1990s: Introduction of supervised and unsupervised learning.
  - 2010s: Emergence of deep learning, enabling AI to handle vast datasets like images and speech.

Age of Artificial Intelligence (AI)

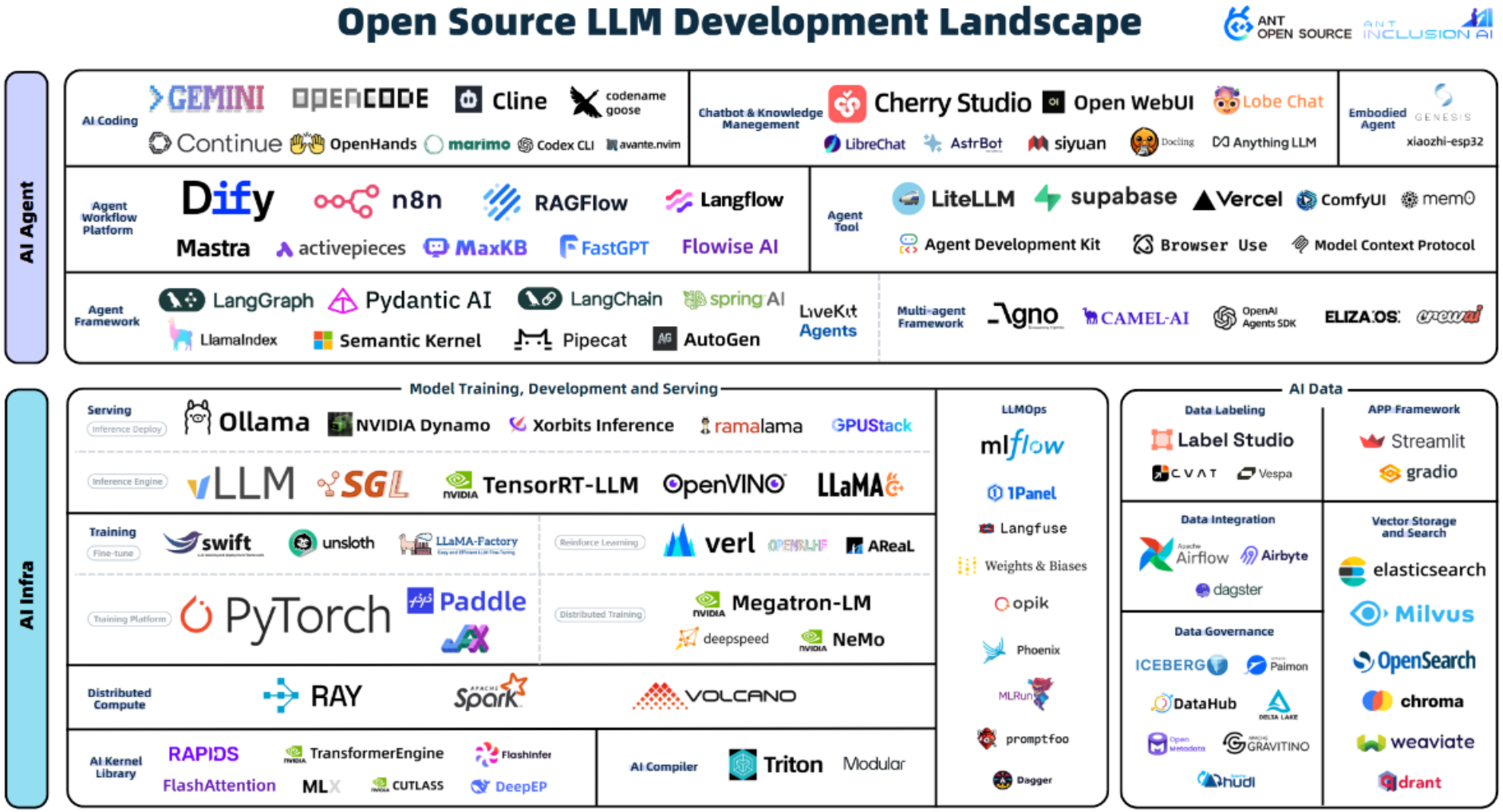




A Brief History of LLM

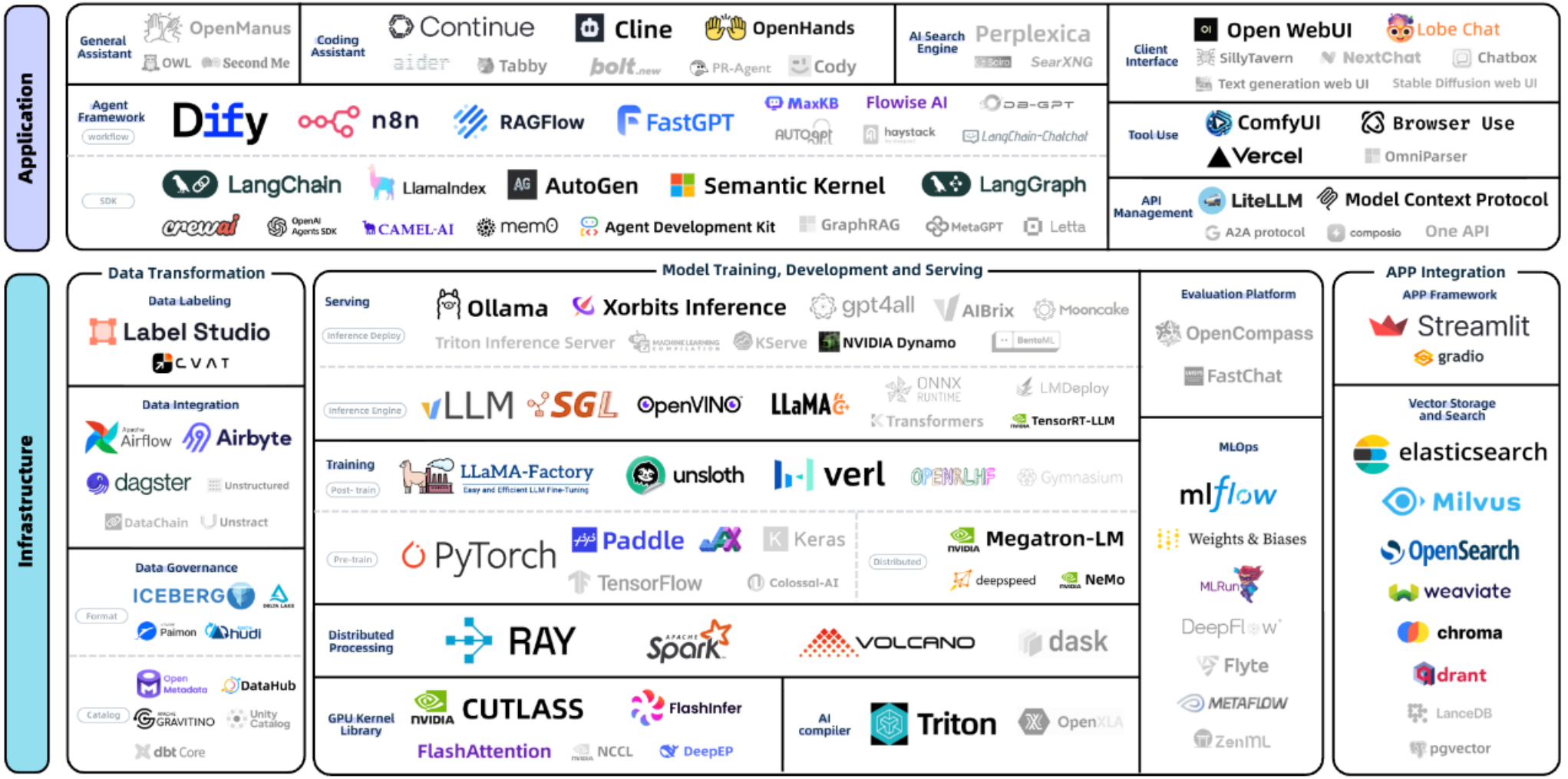


Open Source LLM Development (2025.05)



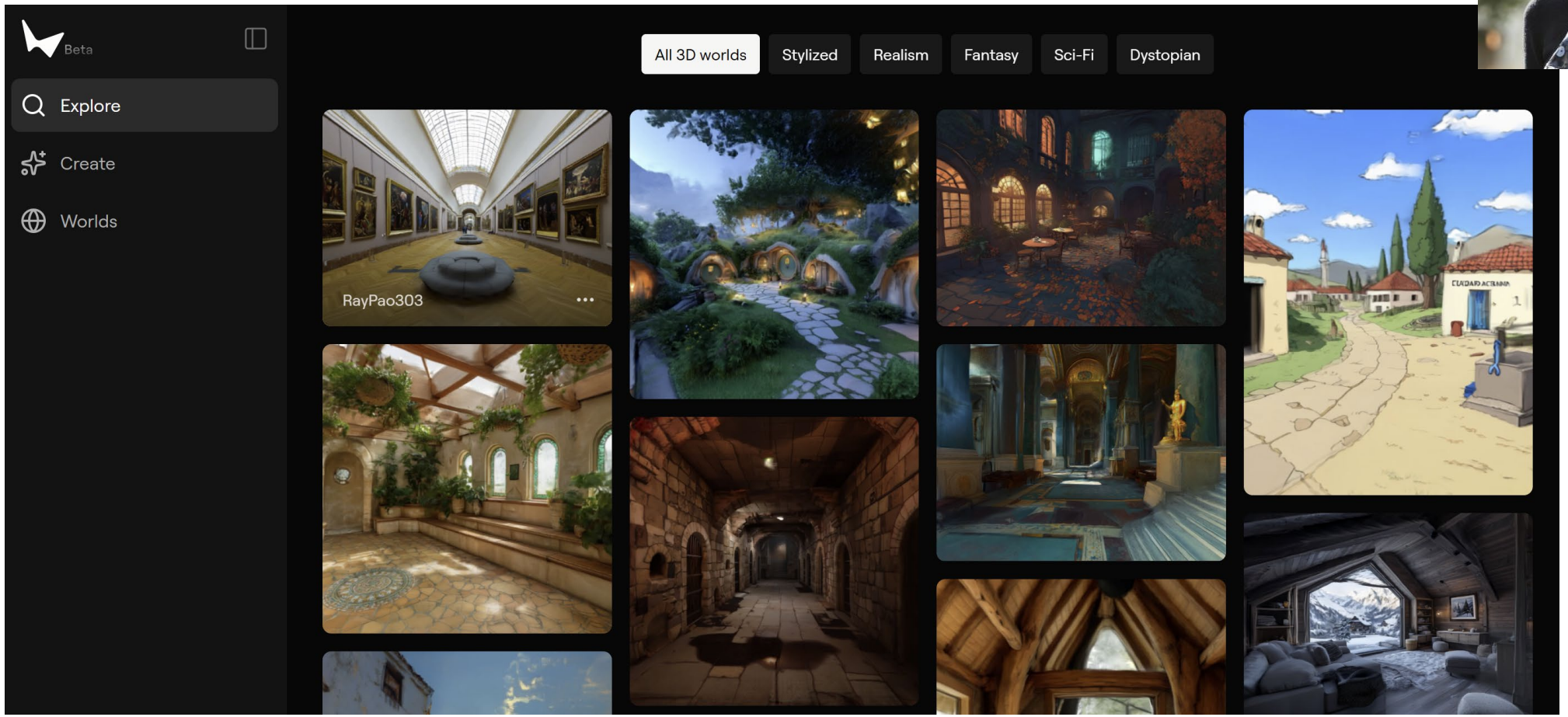
https://github.com/antgroup/llm-oss-landscape

Open Source LLM Development (2025.09)



World Labs: Generate 3D worlds from a single image (Image2World) – Feifei Li

2025.9.17



https://marble.worldlabs.ai/

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

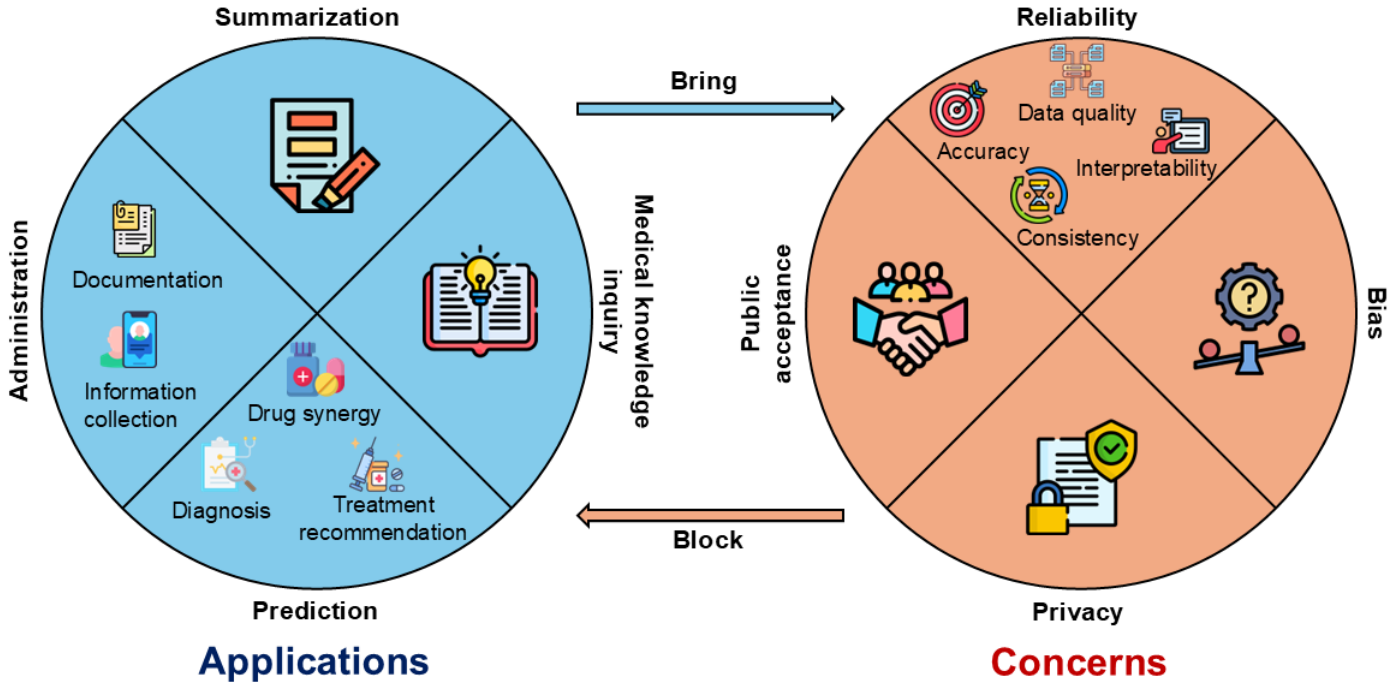
PMCID: PMC6231834 PMID: 30257820

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

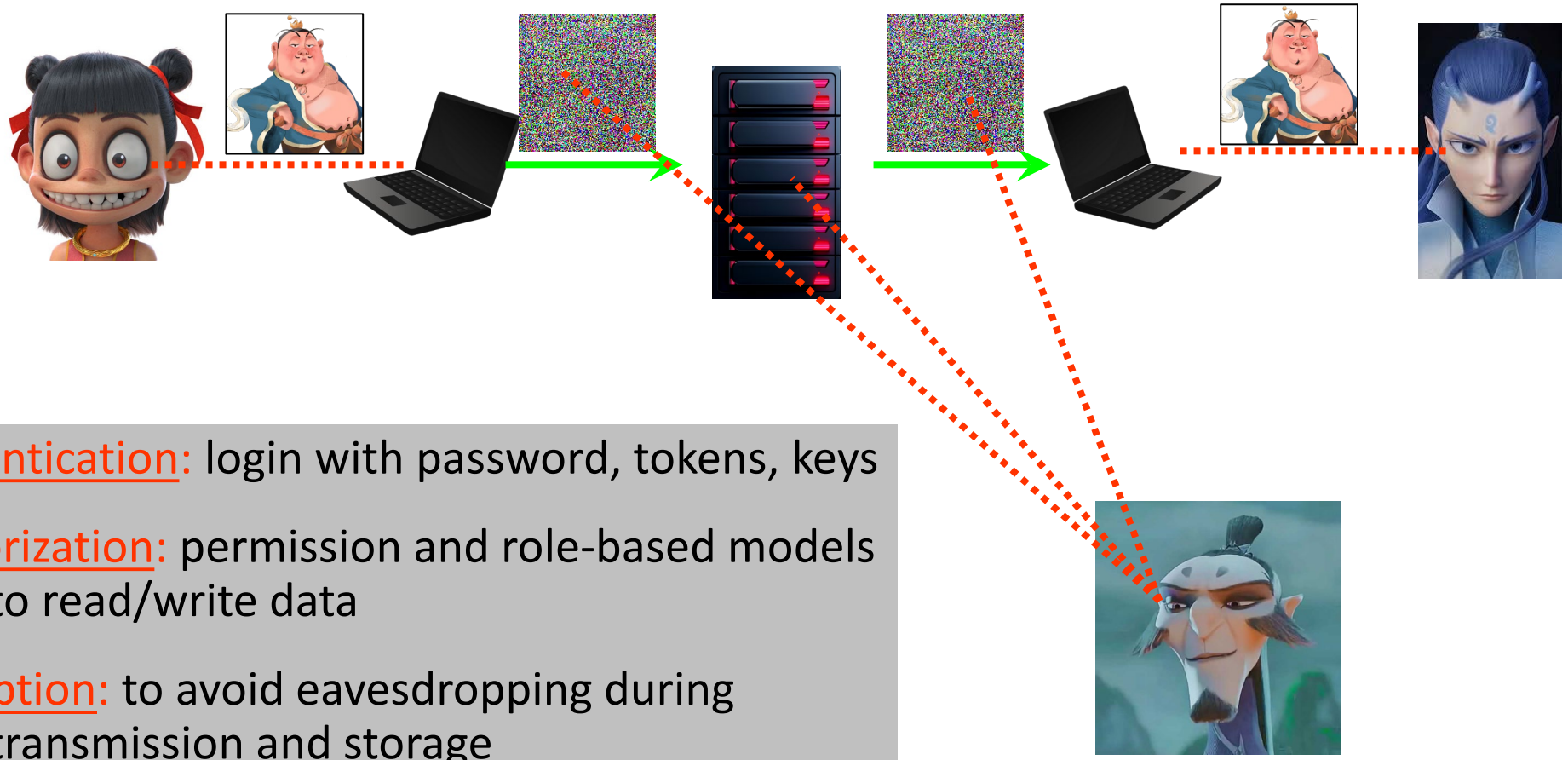
- A summary of the applications and concerns regarding LLMs in healthcare as communicated by 65 reviewed research papers selected from a pool of 820 articles sourced from PubMed, ACM, and IEEE, published before September 1st, 2023.



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?



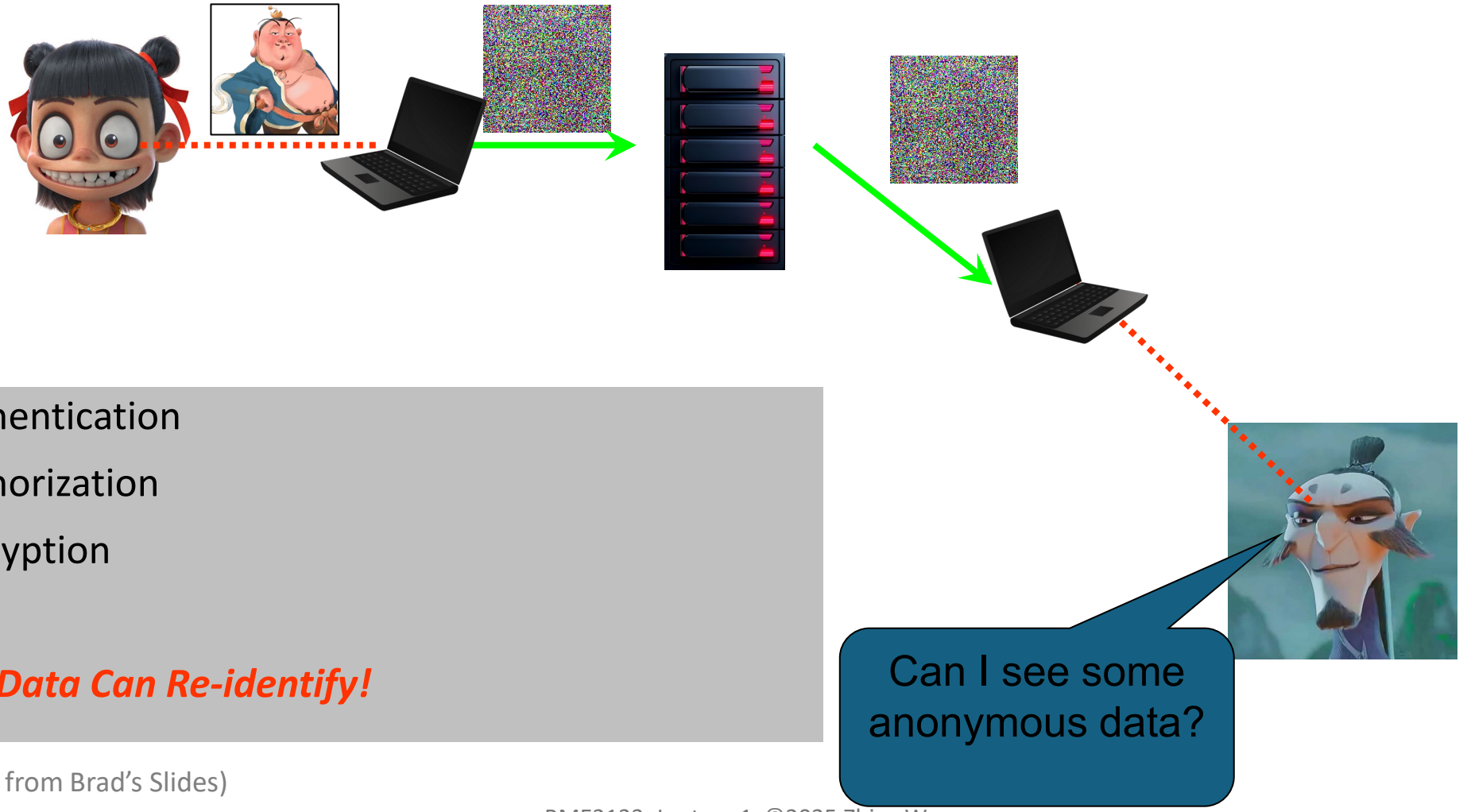
Authentication: login with password, tokens, keys

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?

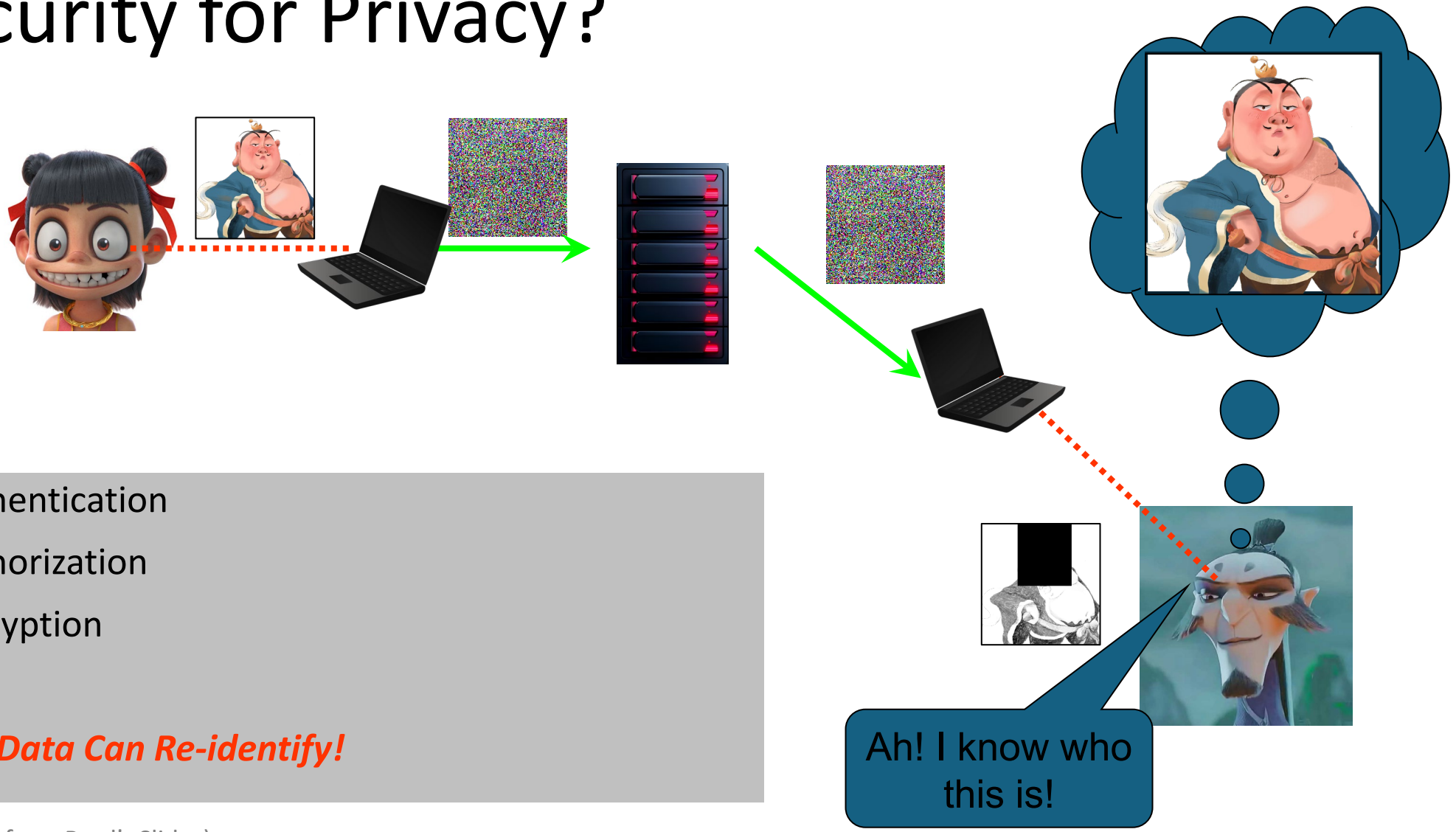


- Authentication
- Authorization
- Encryption

- ***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

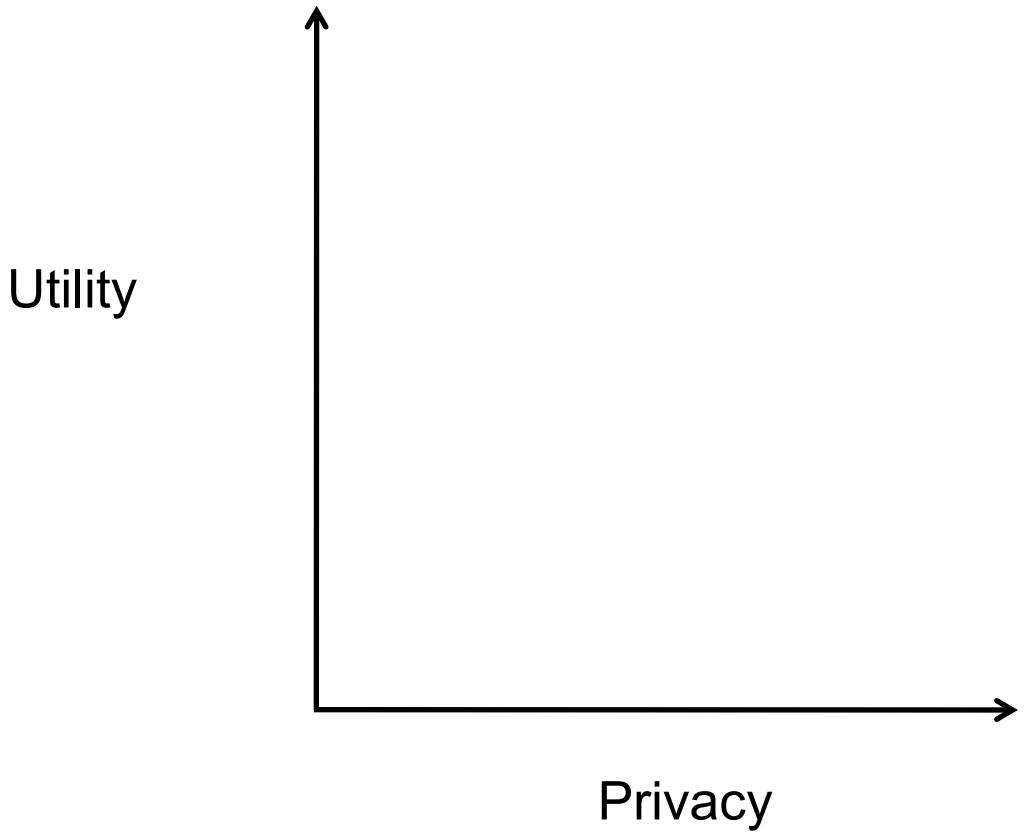
- **Data privacy** is the protection of personal information, ensuring that individuals have control over how their data is collected, used, and shared, while preventing unauthorized access and misuse. (ChatGPT-4o ←"define data privacy in one sentence")
- **Data privacy** is the protection and proper 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

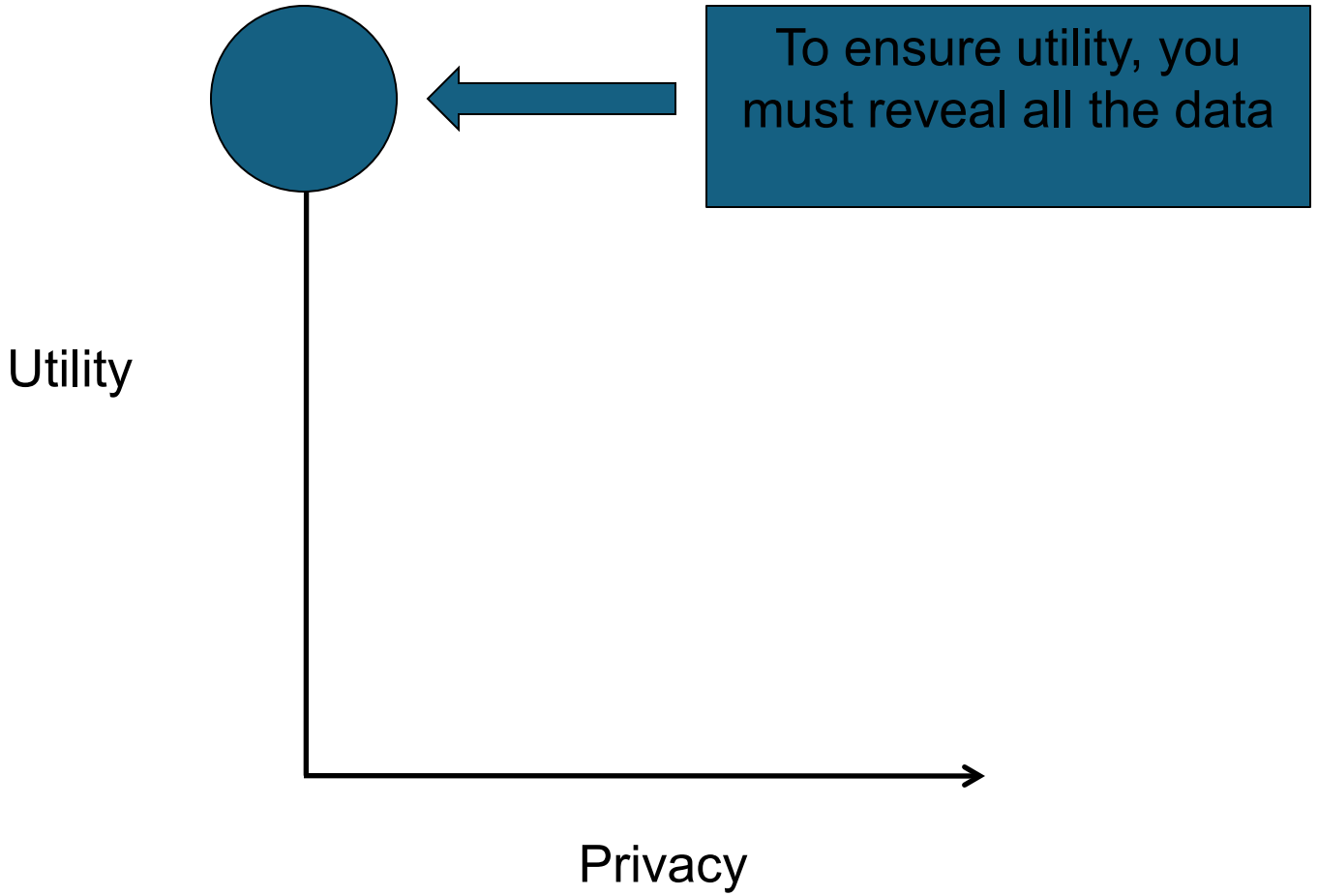
Latanya Sweeney, PhD, FACMI

- 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.**

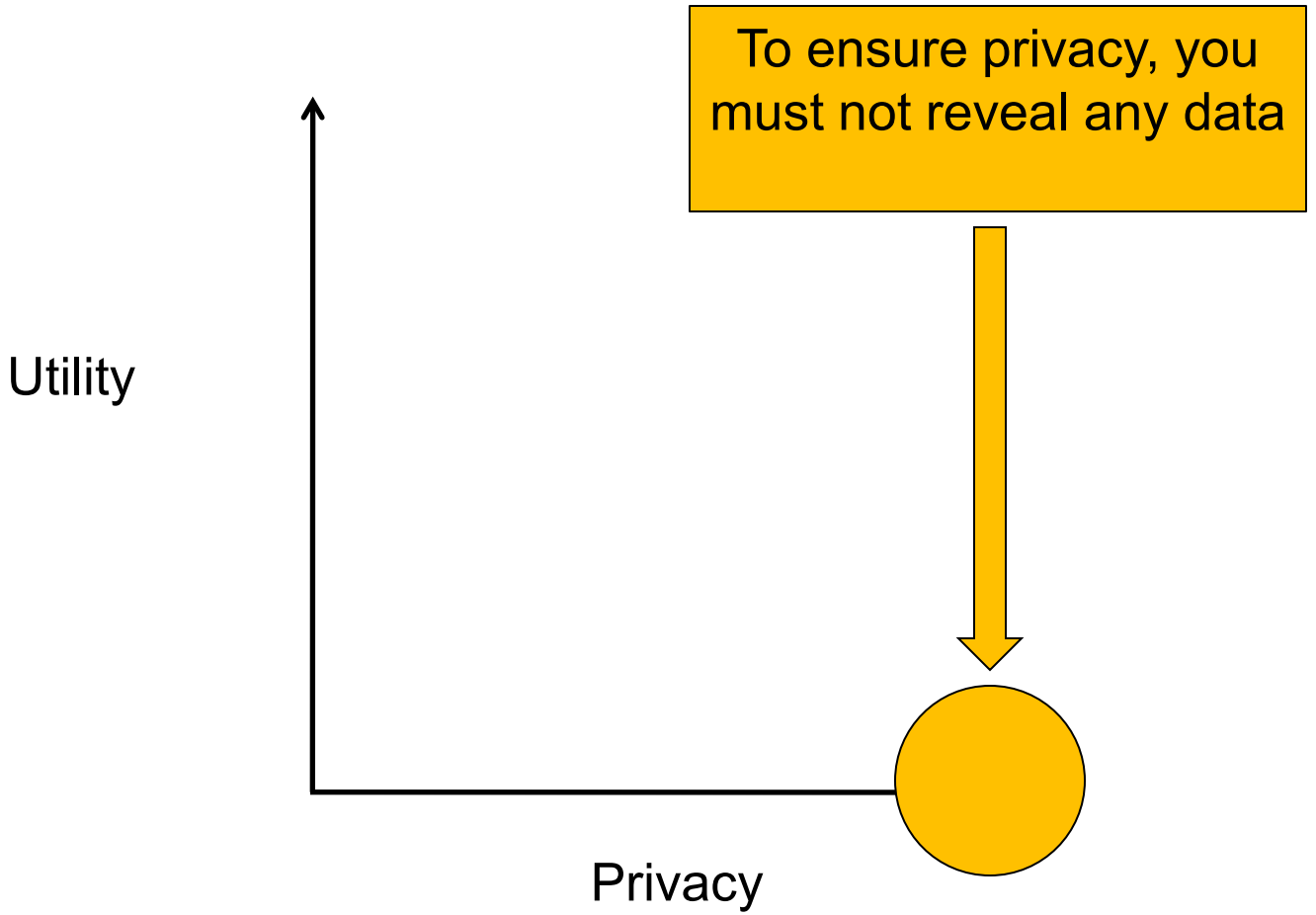
A Visual Perspective



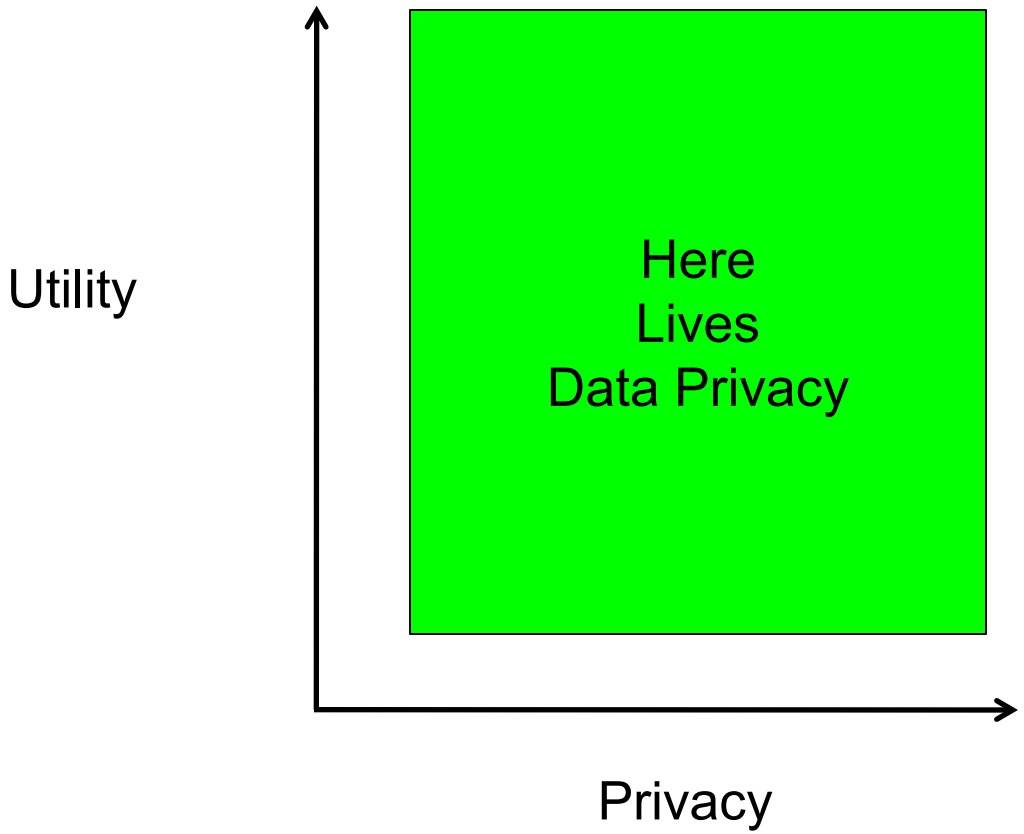
A Visual Perspective



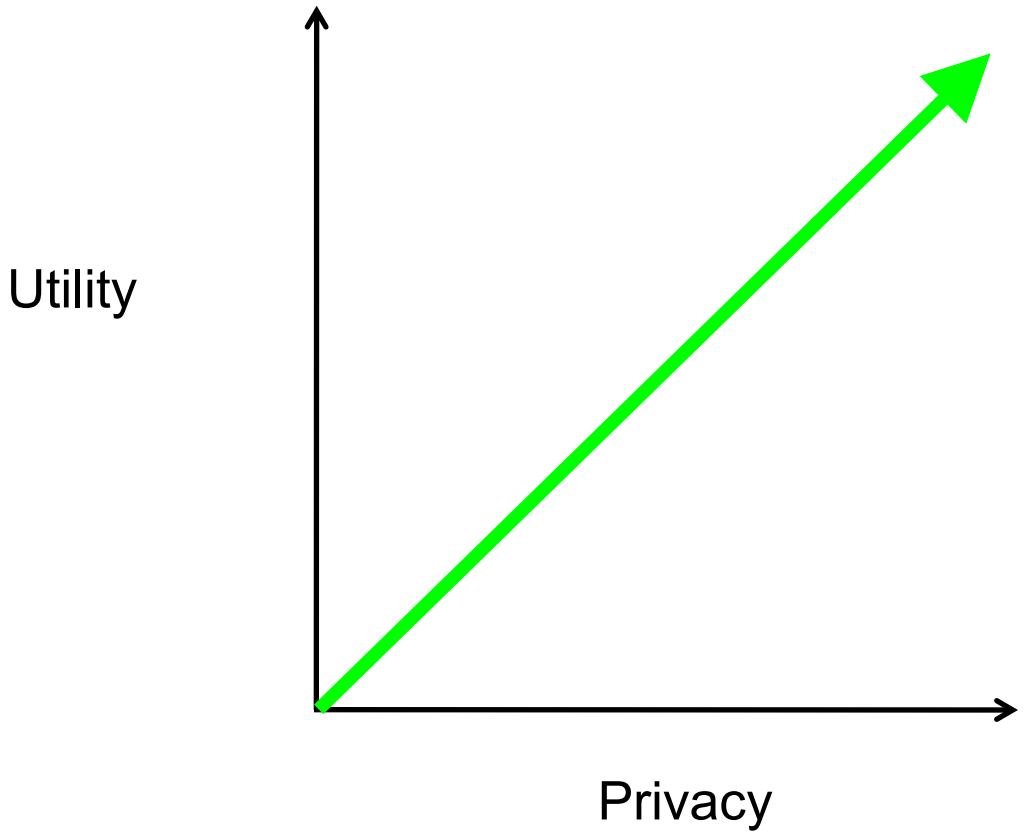
A Visual Perspective



A Visual Perspective

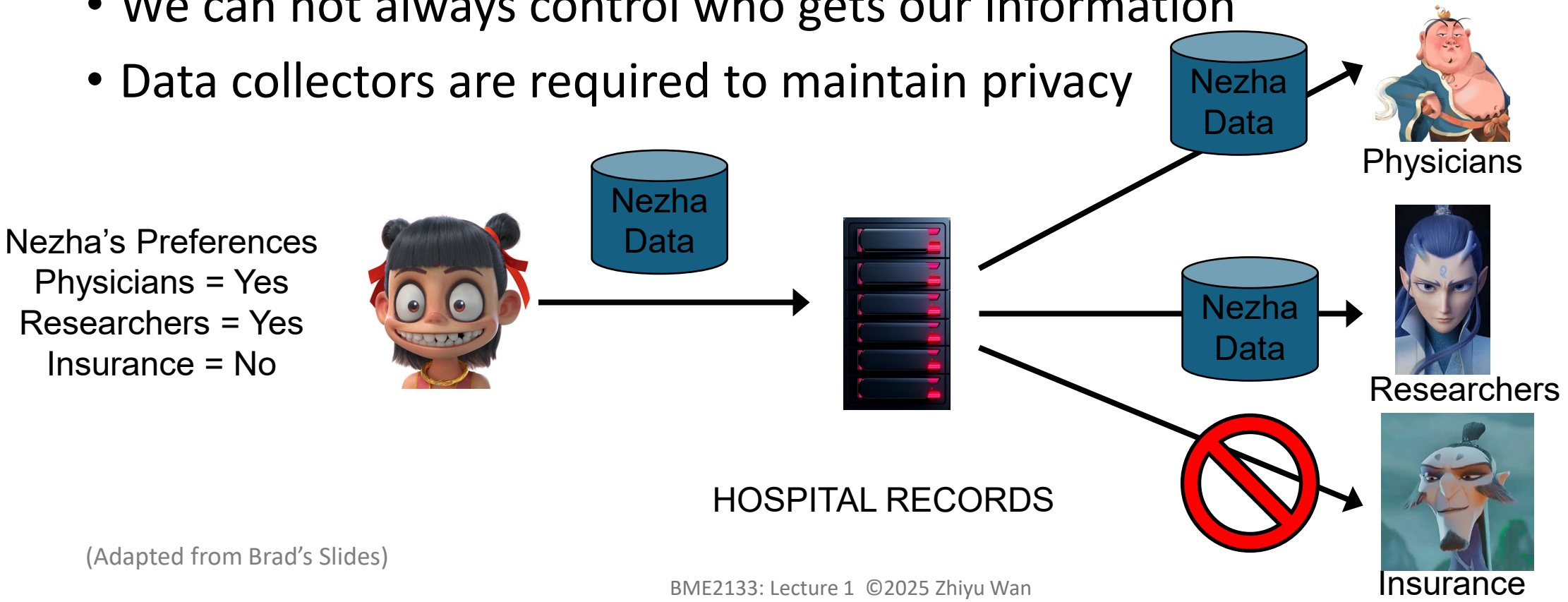


A Visual Perspective



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.