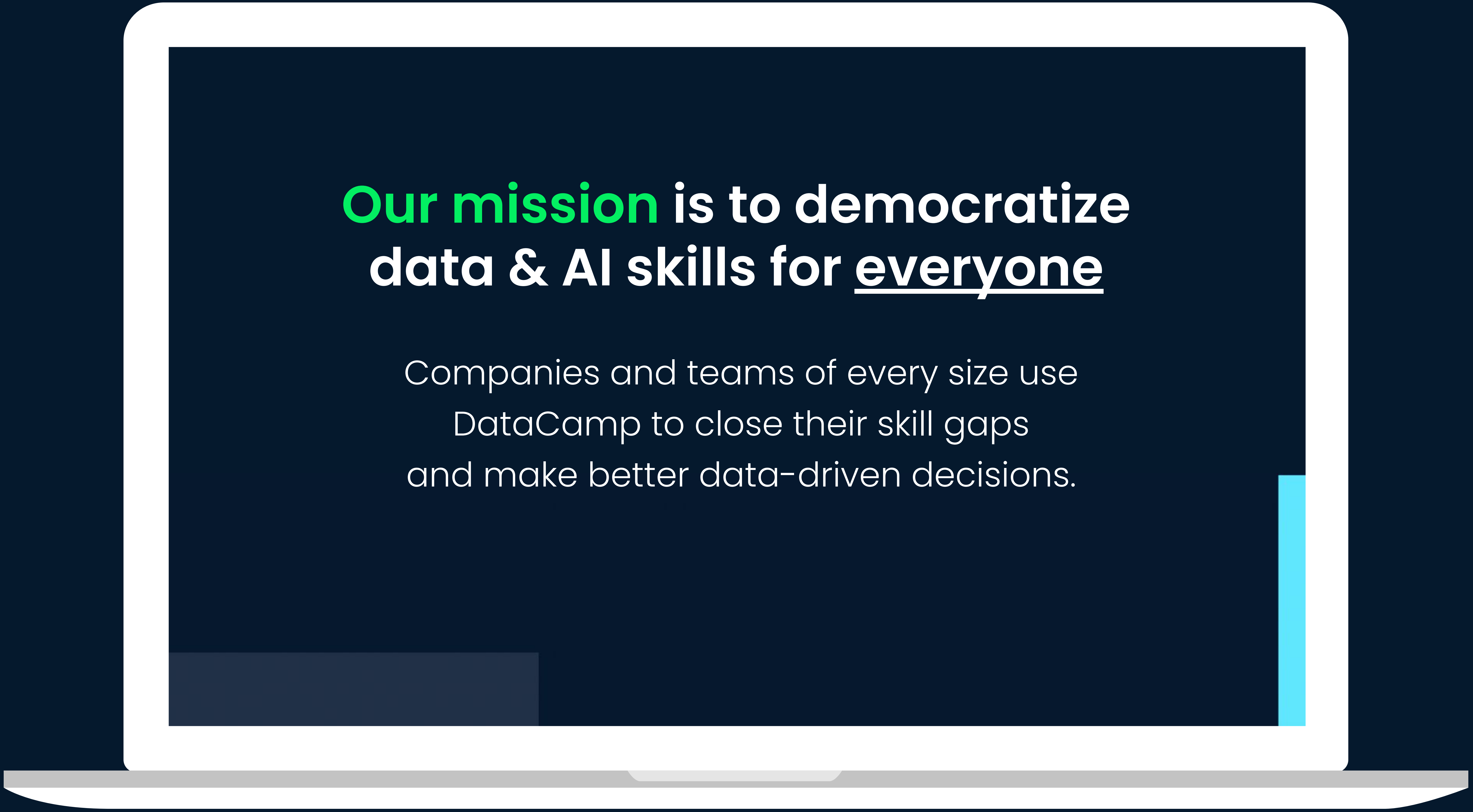
What ChatGPT and Generative AI Mean for Data Privacy

May 11, 2023

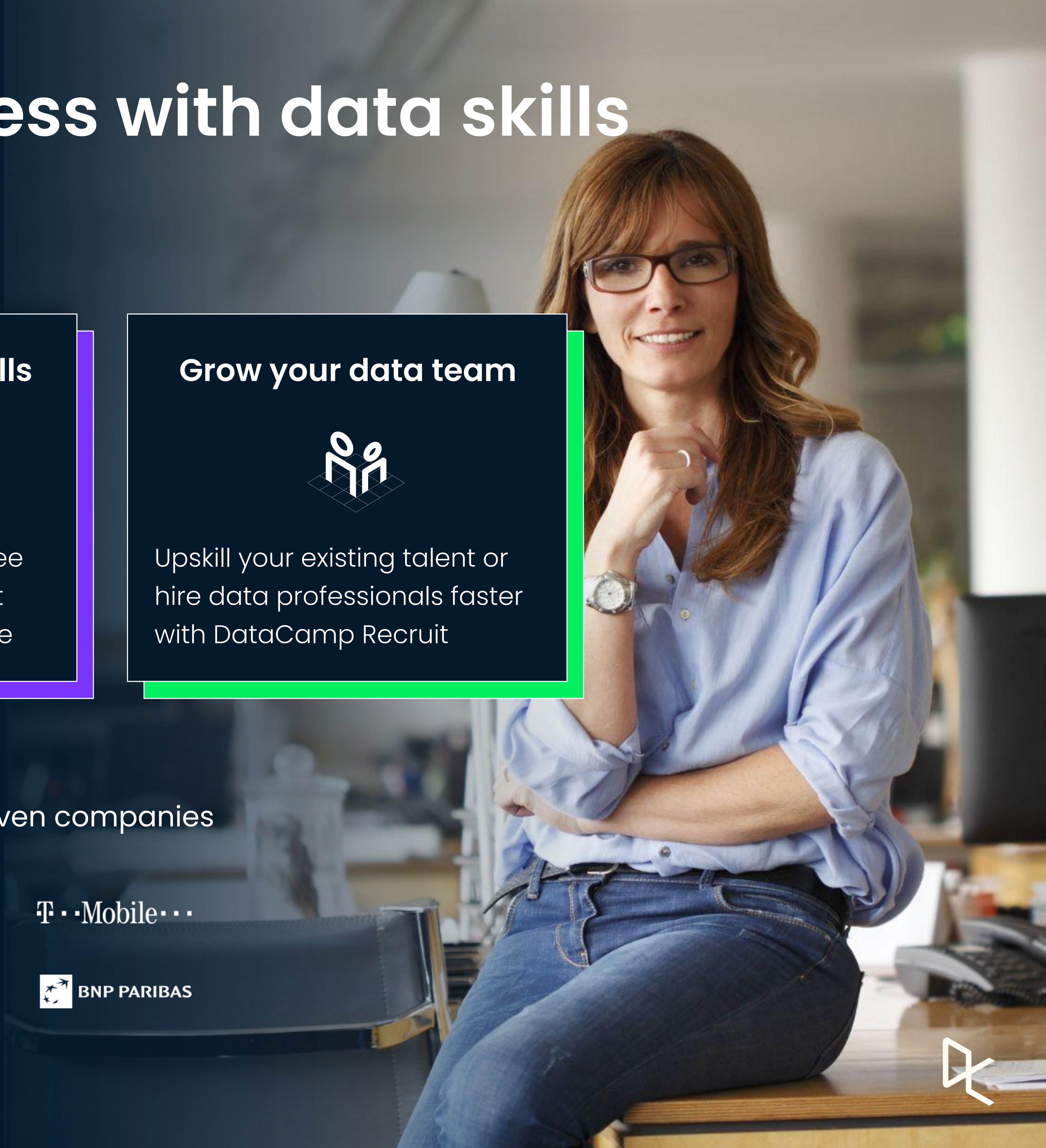
datacamp



Our mission is to democratize data & AI skills for everyone

Companies and teams of every size use
DataCamp to close their skill gaps
and make better data-driven decisions.

Future-proof your business with data skills



Best in class learning

Give your employees access to market-leading training with DataCamp Learn

Build work ready skills

Apply your skills in a risk-free online coding environment with DataCamp Workspace

Grow your data team

Upskill your existing talent or hire data professionals faster with DataCamp Recruit

Trusted by more than 10 million learners and 3,000 data-driven companies

Google Microsoft ebay HSBC COLGATE-PALMOLIVE T··Mobile···

PayPal Uber Deloitte. CREDIT SUISSE Mercedes-Benz BNP PARIBAS

A better webinar experience for you

Ask questions

Open Q&A at the end!

Handouts

We have tons of goodies in the chat section — make sure to check them out!

Share it!

A recording of the webinar will be sent you — make sure to share it with your colleagues!

Hello!

I'm Thad Pitney, General Counsel at DataCamp

Thad Pitney

General Counsel, DataCamp

in tlpitney

Disclaimer

The following presentation is intended for general informational purposes only and does not constitute legal advice or establish an attorney-client relationship. Please note that laws and regulations are subject to change, and the content discussed in this presentation may not reflect the most current legal developments.

While reasonable efforts have been made to ensure the accuracy and reliability of the information presented, the completeness or applicability of the content to specific situations is not guaranteed. Every legal matter is unique, and the information provided may not address your individual circumstances. Therefore, it is advisable to consult with a qualified attorney or legal professional regarding your particular case or legal issue.

Furthermore, this presentation may contain generalizations and simplifications for the purpose of clarity and brevity. The legal concepts discussed are complex, and their application can vary depending on specific jurisdictional and factual nuances. Therefore, you should not rely solely on the information presented herein without seeking professional legal advice.

Any examples mentioned during this presentation are provided for illustrative purposes only and should not be construed as a guarantee or prediction of future legal outcomes.

Lastly, please be aware that communication through this public forum does not establish an attorney-client relationship. Therefore, any information you provide during or after this presentation should not be considered confidential or privileged.

By attending this presentation, you acknowledge and agree to the terms of this disclaimer. If you do not agree with any part of this disclaimer, you should refrain from relying on the information provided and seek legal counsel independently.

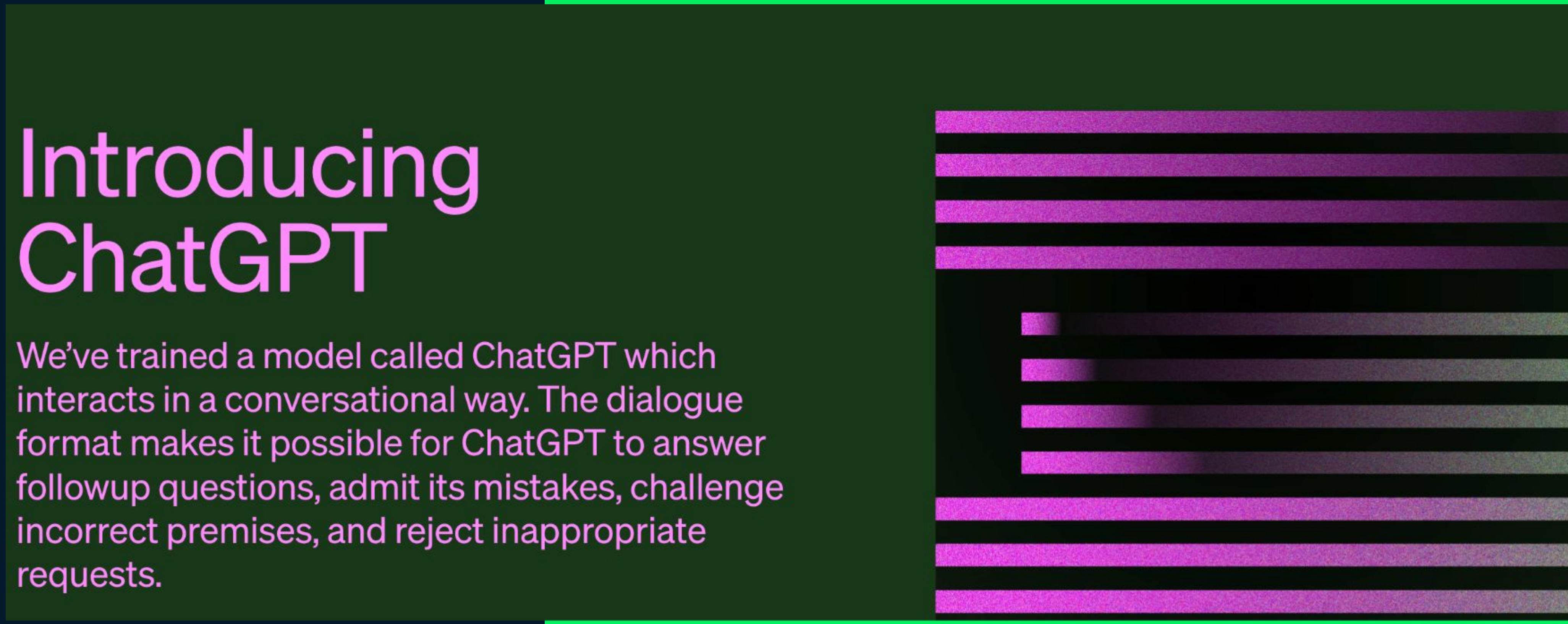
Agenda

1. Generative AI & Common Business Use Cases
2. Overview of Privacy Laws and Principles
3. Intersection of Privacy & AI
4. Addressing AI / Privacy Challenges
5. Who to involve
6. Additional Considerations

1

Generative AI & Common Business Use Cases

AI has exploded in the public consciousness since ChatGPT launched in November 2022



Introducing ChatGPT

We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests.

Lots of uses for generative AI

Training Large Language Models

Using Generative AI APIs in products & services

Using AI tools as part of business activities

✓ Privacy considerations are important in all cases

✓ Important to think about ethics, human rights, fairness / bias

Common Use Cases

1 Customer Support

Instant responses, handling inquiries, FAQs, troubleshooting, and delivering basic product/service information

2 Content Generation & Marketing

Automating content creation, product descriptions, social media content, and personalized email/marketing content

3 Personalized Recommendations

Personalized recommendations for products, services, and content based on user preferences

4 Creative Writing and Storytelling

Idea generation, plot development, and inspiration for writing, storytelling, and scriptwriting

5 Code Generation and Development

Offering suggestions, auto-completion, and contextual recommendations; Accelerates workflows, aids debugging, and facilitates learning new languages/frameworks

2

Overview of Privacy Laws and Principles

Applicable Laws

1 Commonly discussed privacy frameworks

- ✓ *GDPR*
- ✓ *UK Data Protection Act*
- ✓ *CCPA / CPRA*
- ✓ *FTC Act*

2 Many other laws within the US and globally

- ✓ *US Federal: GLBA, HIPAA, FCRA*
- ✓ *US States: Connecticut, Colorado, Virginia*
- ✓ *Global: Australia, Brazil, Canada, China, South Africa and many more*

3 Fair Information Practice Principles (FIPPs)

- ✓ *Many of these laws share a common set of principles known as Fair Information Practice Principles*
- ✓ *Based on recommendations originally proposed by an advisory committee to the US Dept't of Health, Education & Welfare*

Fair Information Practice Principles

1 Collection Limitation

Data collection should be limited, ensuring lawful/fair acquisition and, when applicable, with the consent of the data subject

2 Purpose Specification

Specify the purpose of data collection at time of collection and limit use to fulfilling those purposes or compatible ones

3 Use Limitation

Data should only be used for specified purposes and not for other uses, except with consent or as authorized by law

4 The Data Quality Principle

Data should be relevant, accurate, complete, and kept up-to-date

5 Openness

Ensure a means for individuals to easily ascertain the existence, nature, main purposes of use, and identity of the data controller

Fair Information Practice Principles

6 Individual Participation

Individuals have the right to

- ✓ *Confirm whether a data controller holds their data*
- ✓ *Access their data*
- ✓ *Receive reasons if their request is denied and the ability to challenge the denial;*
- ✓ *Challenge and, if successful, have their data erased or corrected.*

7 Security Safeguards

Data should have reasonable security safeguards protect against unauthorized access, loss, destruction, modification, or disclosure

8 Accountability

Data controllers should be accountable for implementing measures that ensure compliance with the principlesç

AI Privacy Principles

1 Guidelines for AI development

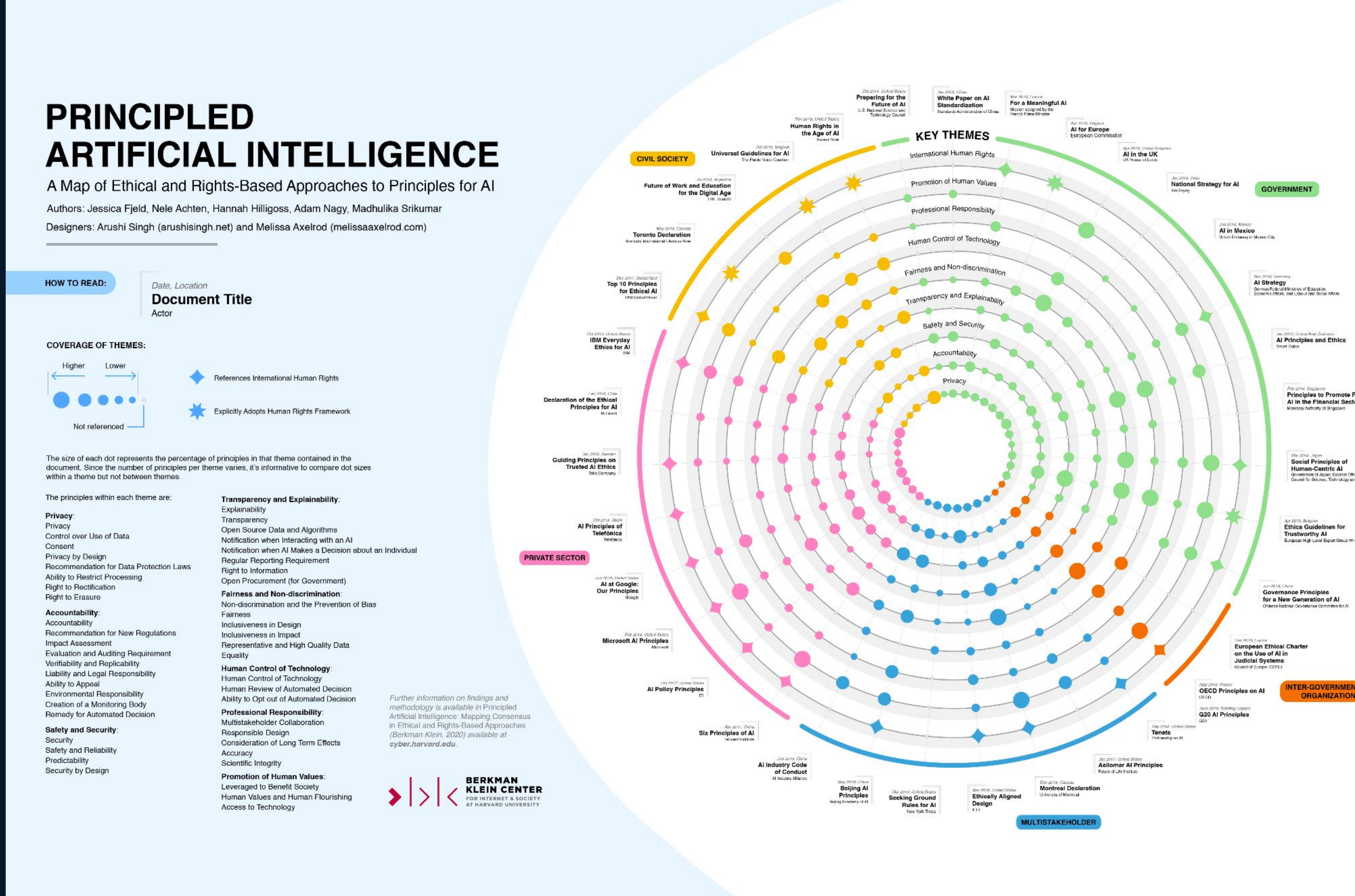
Proposed by a number of different sources (UNESCO, OECD, Council of Europe, European Commission)

2 Substantial overlap with FIPPs

✓ *Privacy (includes control over use of data, rights to erasure and correction, consent)*

✓ *Accountability (includes liability and legal responsibility)*

✓ *Security (includes safety and reliability)*



PRINCIPLED ARTIFICIAL INTELLIGENCE

A Map of Ethical and Rights-Based Approaches to Principles for AI

Authors: Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar

Designers: Arushi Singh (arushisingh.net) and Melissa Axelrod (melissaaxelrod.com)

HOW TO READ:

Date, Location
Document Title
Actor

COVERAGE OF THEMES:

Higher ← → Lower
Not referenced

◆ References International Human Rights

✸ Explicitly Adopts Human Rights Framework

The size of each dot represents the percentage of principles in that theme contained in the document. Since the number of principles per theme varies, it's informative to compare dot sizes within a theme but not between themes.

The principles within each theme are:

Privacy:
Privacy
Control over Use of Data
Consent
Privacy by Design
Recommendation for Data Protection Laws
Ability to Restrict Processing
Right to Rectification
Right to Erasure

Accountability:
Accountability
Recommendation for New Regulations
Impact Assessment
Evaluation and Auditing Requirement
Verifiability and Replicability
Liability and Legal Responsibility
Ability to Appeal
Environmental Responsibility
Creation of a Monitoring Body
Remedy for Automated Decision

Safety and Security:
Security
Safety and Reliability
Predictability
Security by Design

Transparency and Explainability:
Explainability
Transparency
Open Source Data and Algorithms
Notification when Interacting with an AI
Notification when AI Makes a Decision about an Individual
Regular Reporting Requirement
Right to Information
Open Procurement (for Government)

Fairness and Non-discrimination:
Non-discrimination and the Prevention of Bias
Fairness
Inclusiveness in Design
Inclusiveness in Impact
Representative and High Quality Data
Equality

Human Control of Technology:
Human Control of Technology
Human Review of Automated Decision
Ability to Opt out of Automated Decision

Professional Responsibility:
Multistakeholder Collaboration
Responsible Design
Consideration of Long Term Effects
Accuracy
Scientific Integrity

Promotion of Human Values:
Leveraged to Benefit Society
Human Values and Human Flourishing
Access to Technology

Further information on findings and methodology is available in Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches *(Berkman Klein, 2020) available at* ***cyber.harvard.edu***.

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

KEY THEMES
International Human Rights
Promotion of Human Values
Professional Responsibility
Human Control of Technology
Fairness and Non-discrimination
Transparency and Explainability
Safety and Security
Accountability
Privacy
CIVIL SOCIETY
GOVERNMENT
PRIVATE SECTOR
MULTISTAKEHOLDER
INTER-GOVERNMEN ORGANIZATION
Oct 2016, United States Preparing for the Future of AI U.S. National Science and Technology Council
Jan 2018, China White Paper on AI Standardization Standards Administration of China
Mar 2018, France For a Meaningful AI Mission assigned by the French Prime Minister
Apr 2018, Belgium AI for Europe European Commission
Apr 2018, United Kingdom AI in the UK UK House of Lords
Jun 2018, India National Strategy for AI Niti Aayog
Jun 2018, Mexico AI in Mexico British Embassy in Mexico City
Nov 2018, Germany AI Strategy German Federal Ministries of Education, Economic Affairs, and Labour and Social Affairs
Jan 2019, United Arab Emirates AI Principles and Ethics Smart Dubai
Feb 2019, Singapore Principles to Promote F AI in the Financial Secto Monetary Authority of Singapore
Mar 2019, Japan Social Principles of Human-Centric AI Government of Japan; Cabinet Offi Council for Science, Technology an
Apr 2019, Belgium Ethics Guidelines for Trustworthy AI European High Level Expert Group on
Jun 2019, China Governance Principles for a New Generation of AI Chinese National Governance Committee for AI
Dec 2018, France European Ethical Charter on the Use of AI in Judicial Systems Council of Europe: CEPEJ
May 2019, France OECD Principles on AI OECD
June 2019, Rotating (Japan) G20 AI Principles G20
Sep 2016, United States Tenets Partnership on AI
Jan 2017, United States Asilomar AI Principles Future of Life Institute
Dec 2018, Canada Montreal Declaration University of Montreal
Mar 2019, United States Ethically Aligned Design IEEE
Mar 2019, United States Seeking Ground Rules for AI New York Times
May 2019, China Beijing AI Principles Beijing Academy of AI
Jun 2019, China AI Industry Code of Conduct AI Industry Alliance
Apr 2017, China Six Principles of AI Tencent Institute
Oct 2017, United States AI Policy Principles ITI
Feb 2018, United States Microsoft AI Principles Microsoft
Jun 2018, United States AI at Google: Our Principles Google
Oct 2018, Spain AI Principles of Telefónica Telefónica
Jan 2019, Sweden Guiding Principles on Trusted AI Ethics Telia Company
Feb 2019, Chile Declaration of the Ethical Principles for AI IA Latam
Oct 2018, United States IBM Everyday Ethics for AI IBM
Dec 2017, Switzerland Top 10 Principles for Ethical AI UNI Global Union
May 2018, Canada Toronto Declaration Amnesty International | Access Now
Jul 2018, Argentina Future of Work and Education for the Digital Age T20: Think20
Oct 2018, Belgium Universal Guidelines for AI The Public Voice Coalition
Nov 2018, United States Human Rights in the Age of AI Access Now

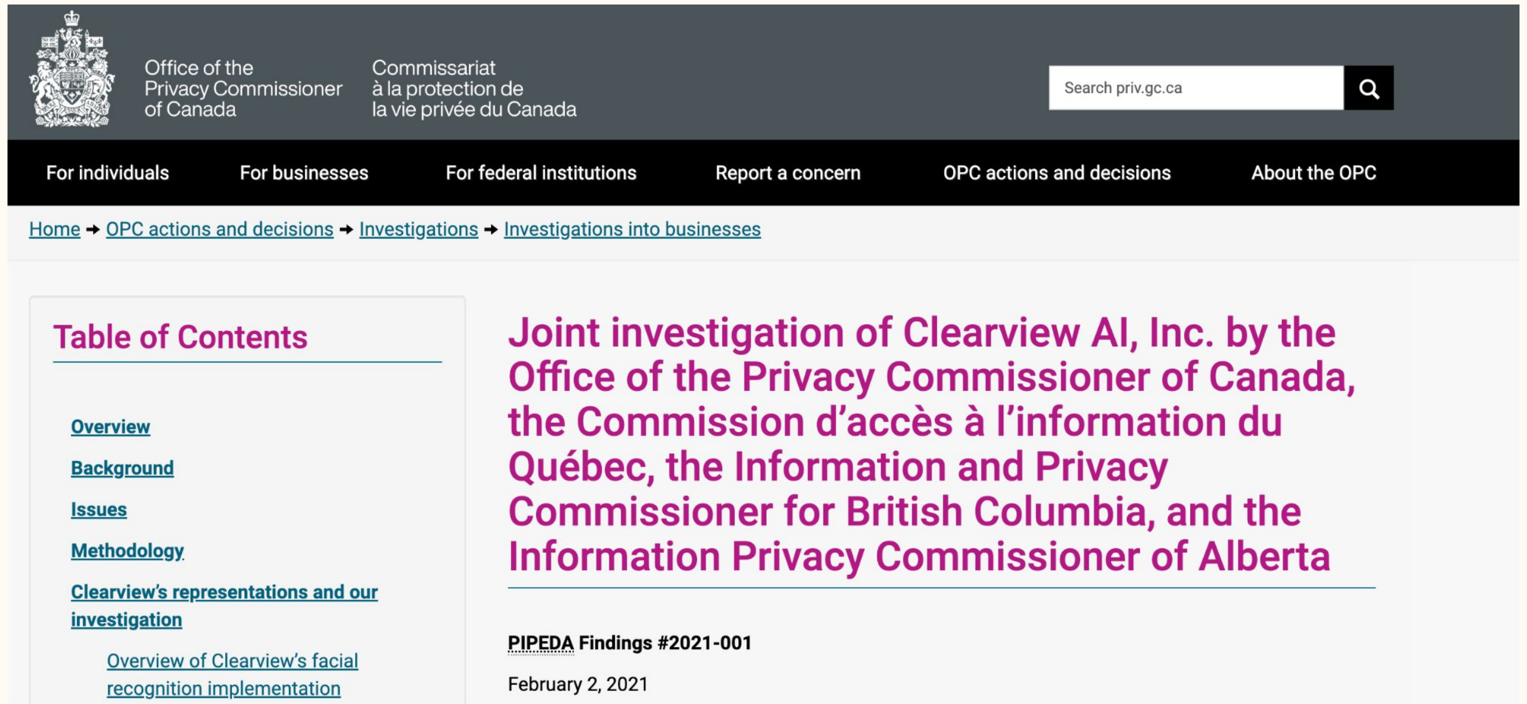
3

Intersection of Privacy & AI

Consent and purpose of data collection

Concern: Data used in AI models outside the purpose for which it was originally collected

Clearview AI



Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada
Search priv.gc.ca
For individuals
For businesses
For federal institutions
Report a concern
OPC actions and decisions
About the OPC
Home → OPC actions and decisions → Investigations → Investigations into businesses

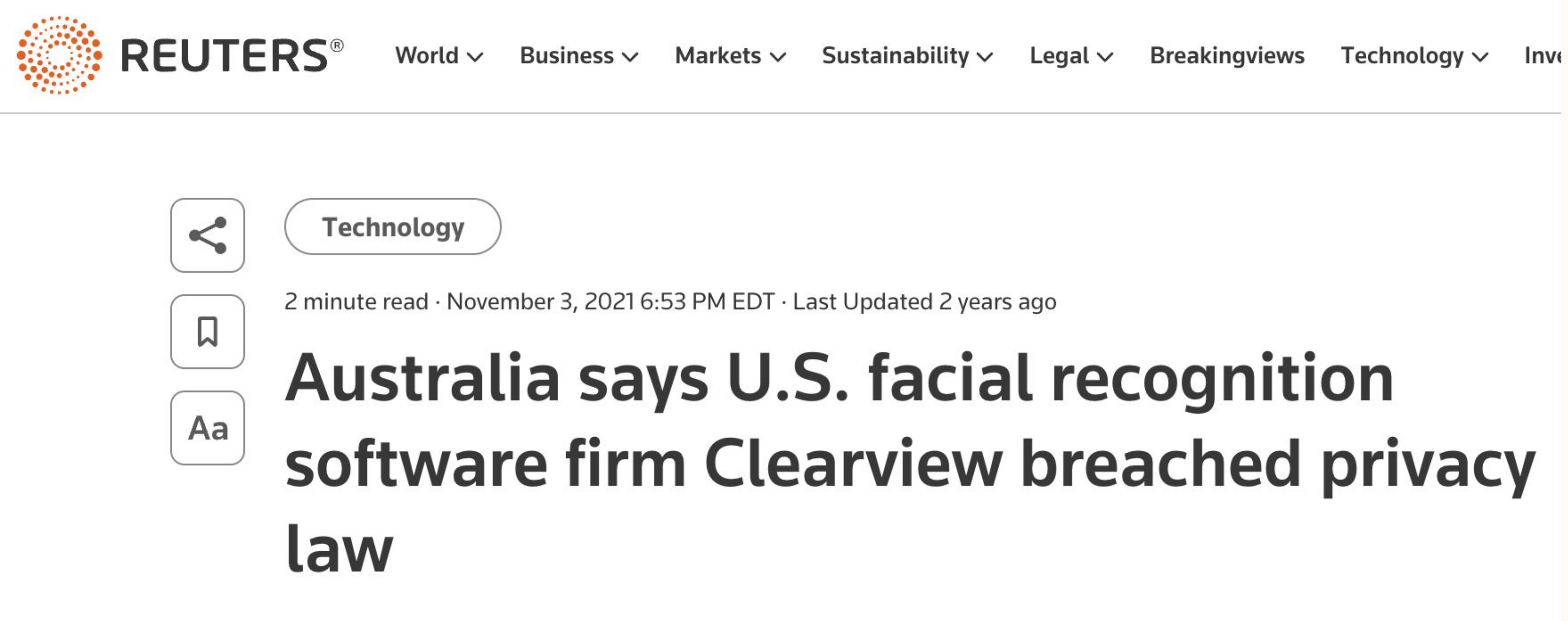
Table of Contents

- Overview
- Background
- Issues
- Methodology
- Clearview's representations and our investigation
  - Overview of Clearview's facial recognition implementation

Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta

PIPEDA Findings #2021-001

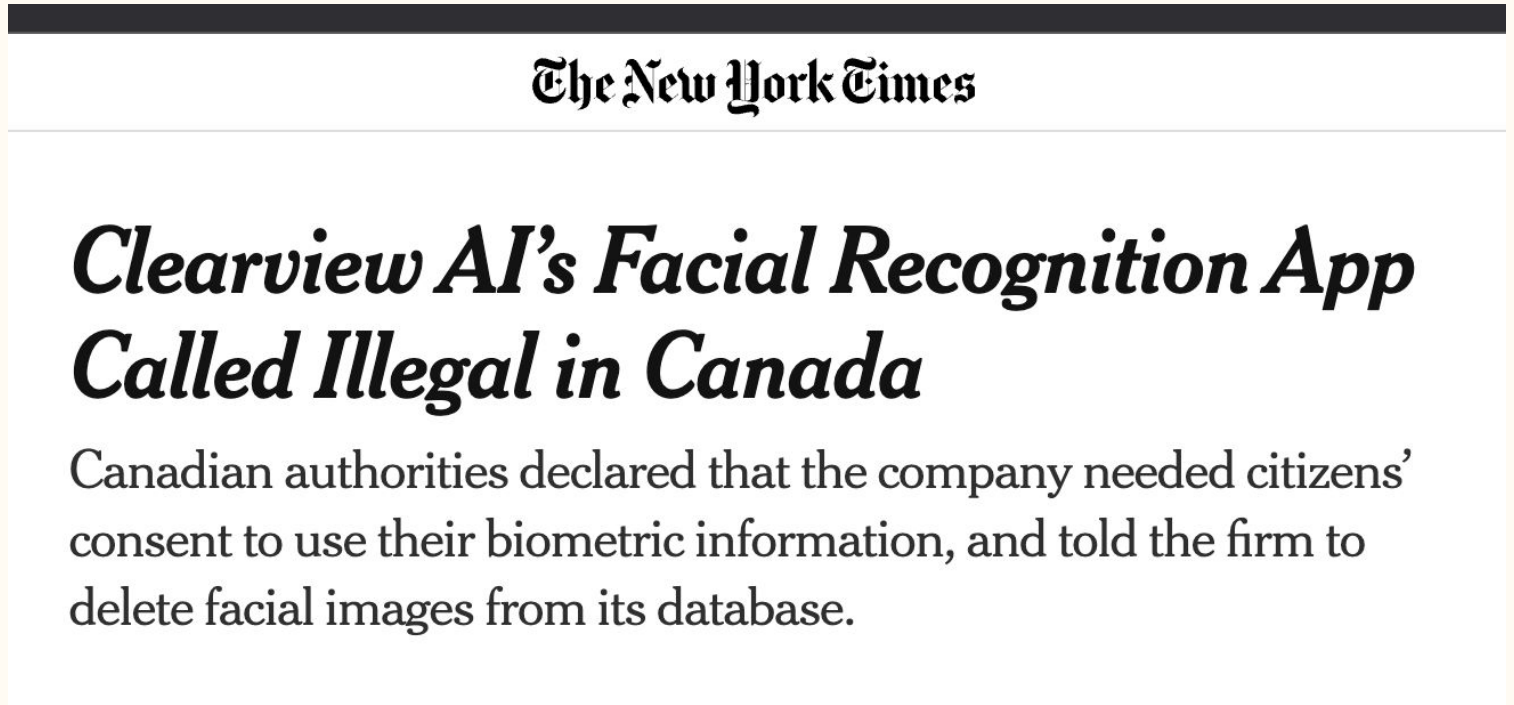
February 2, 2021



Technology

2 minute read · November 3, 2021 6:53 PM EDT · Last Updated 2 years ago

Australia says U.S. facial recognition software firm Clearview breached privacy law



Clearview AI's Facial Recognition App Called Illegal in Canada

Canadian authorities declared that the company needed citizens' consent to use their biometric information, and told the firm to delete facial images from its database.

Concern: Data used in AI models outside the purpose for which it was originally collected

- ✓ Clearview built a facial recognition database using images collected from social media sites (among other sources) without the knowledge or consent of individuals. Clearview sold access to the technology to, among others, law enforcement agencies
- ✓ Faced multiple investigations and lawsuits (Australia, Canada, UK, US)
- ✓ Clearview's practices were deemed illegal in Canada and Australia among other locations. The company continues to face substantial privacy related fines, particularly in the EU

Persistence & right to be forgotten

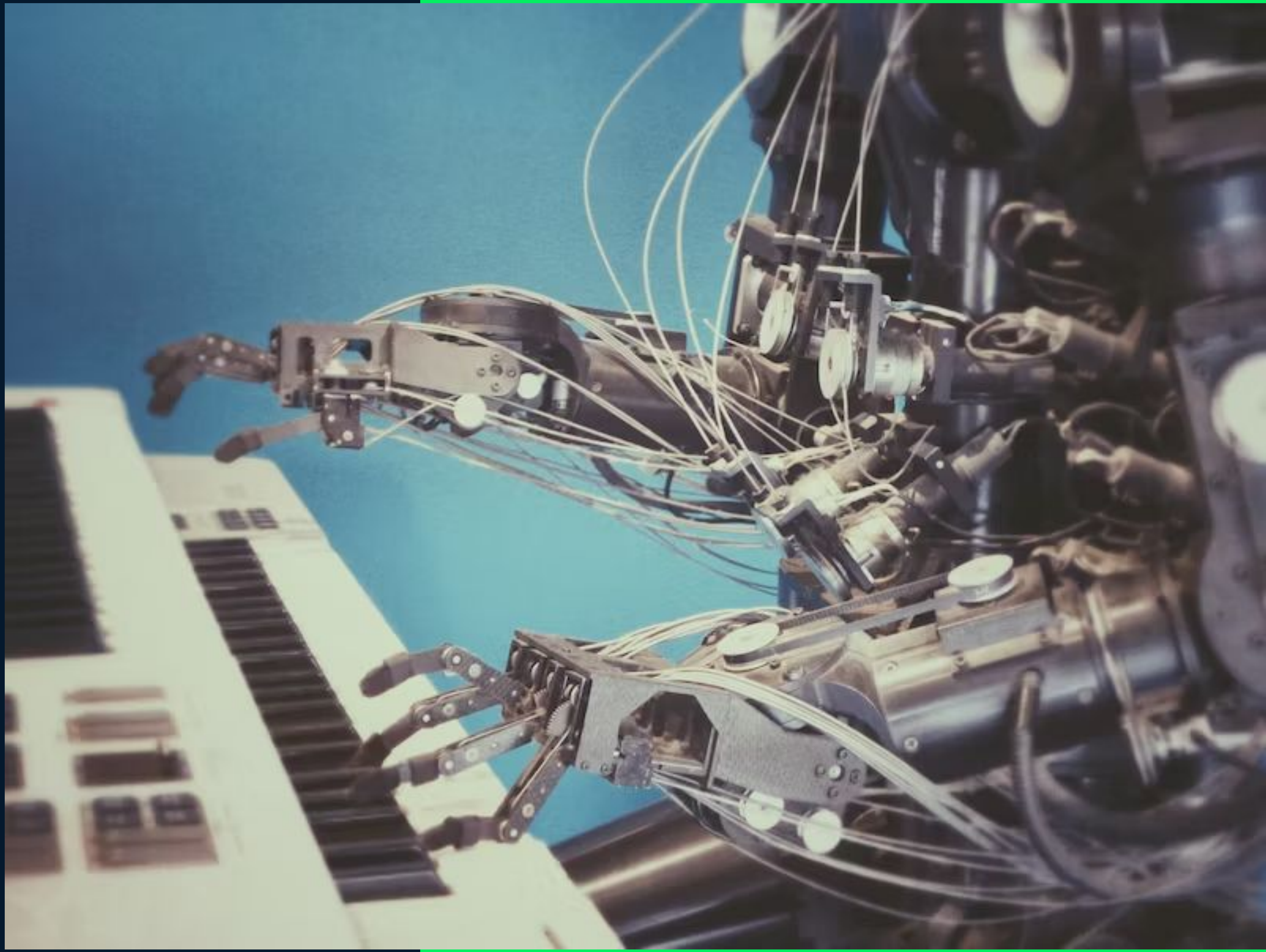
Concern: Use of personal data in large language models complicates an individual's right to be forgotten

Persistence & right to be forgotten

Concern: Use of personal data in large language models complicates an individual's right to be forgotten

- ✓ Organizations training large language models are unlikely to have comprehensive knowledge of all the data in the training dataset
- ✓ Language models typically retain information learned during training, even if the specific training data is removed.
- ✓ Possible solutions
  - ○ Retraining
  - ○ Replacing with synthetic data
  - ○ Machine unlearning

Automated Decision-making



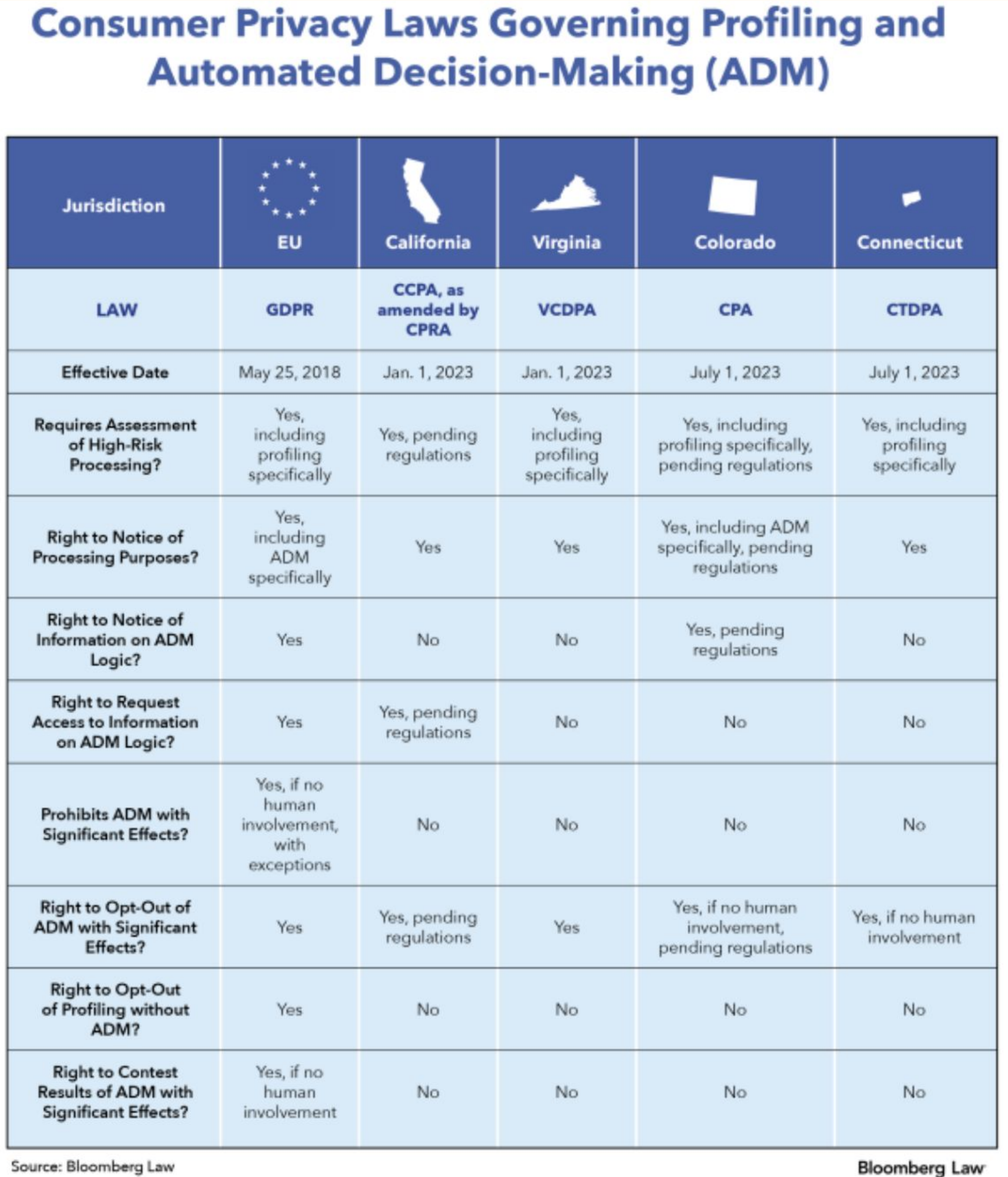
Automated Decision Making

What are some automated decisions

- ✓ Customer support
- ✓ Data Analysis & Insights
- ✓ Compliance
- ✓ Application Processing

Right to Explanation

- ✓ GDPR Article 22 and other laws
- ✓ Individuals have the right to meaningful information about the logic, significance, and consequences of the automated decision-making process
- ✓ Applies to decisions that produce legal effects or similarly significant effects solely based on automated processing



Consumer Privacy Laws Governing Profiling and Automated Decision-Making (ADM)

Jurisdiction	EU	California	Virginia	Colorado	Connecticut
LAW	GDPR	CCPA, as amended by CPRA	VCDPA	CPA	CTDPA
Effective Date	May 25, 2018	Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	July 1, 2023
Requires Assessment of High-Risk Processing?	Yes, including profiling specifically	Yes, pending regulations	Yes, including profiling specifically	Yes, including profiling specifically, pending regulations	Yes, including profiling specifically
Right to Notice of Processing Purposes?	Yes, including ADM specifically	Yes	Yes	Yes, including ADM specifically, pending regulations	Yes
Right to Notice of Information on ADM Logic?	Yes	No	No	Yes, pending regulations	No
Right to Request Access to Information on ADM Logic?	Yes	Yes, pending regulations	No	No	No
Prohibits ADM with Significant Effects?	Yes, if no human involvement, with exceptions	No	No	No	No
Right to Opt-Out of ADM with Significant Effects?	Yes	Yes, pending regulations	Yes	Yes, if no human involvement, pending regulations	Yes, if no human involvement
Right to Opt-Out of Profiling without ADM?	Yes	No	No	No	No
Right to Contest Results of ADM with Significant Effects?	Yes, if no human involvement	No	No	No	No

Source: Bloomberg Law

Bloomberg Law

Automated Decision Making

Compliance with Explanation and Transparency Requirements

- ✓ Provide individuals with clear and understandable information about the logic, significance, and consequences of automated decisions

- ✓ The explainability issue — The complexity of algorithms can make it challenging to understand the rationale behind an automated decision

Automated Decision Making

Compliance with Explanation and Transparency Requirements

✓ At a minimum organizations should consider:
  - Clearly communicating that the decisions are driven by a large language model and explain the model's purpose, capabilities, and limitations.
  - Providing documentation outlining the model's architecture, training data sources, and any preprocessing or filtering steps applied to the data and detailing the algorithms and methodologies used for decision-making
  - Describing how the input provided to the model is transformed into a decision and explain the factors considered by the model in generating a response

✓ Other steps that could be included:
  - Model behavior
  - Testing and validation
  - Human oversight and intervention (separately required under GDPR)
  - Feedback mechanisms and continuous improvement commitments

4

Addressing AI / Privacy Challenges

Avoiding AI Privacy Issues

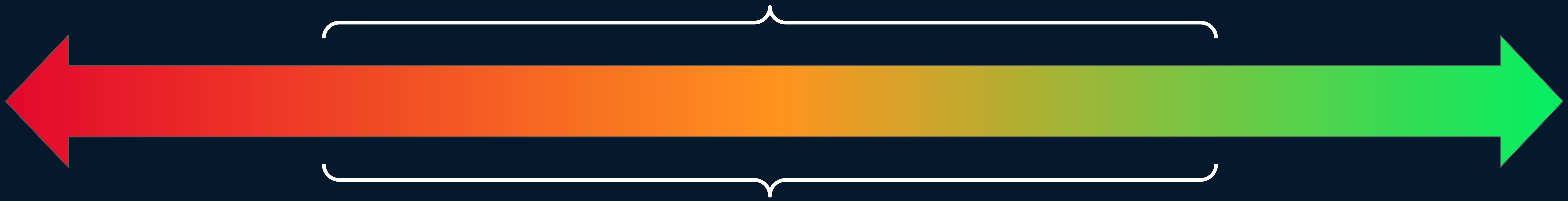
1 Implications of AI can be seen as an extension of those created by big data

But AI also to uses data to learn, develop adaptive models and make actionable predictions

2 Strategies to minimize risk are also largely similar

- ✓ *Data Minimization*
- ✓ *Privacy by Design*
- ✓ *Informed Consent*
- ✓ *Data Security*
- ✓ *Privacy Impact Assessments*
- ✓ *Transparency and Explainability*
- ✓ *User Controls and Rights*
- ✓ *Ethical Guidelines and Standards*
- ✓ *Regular Audits and Compliance*
- ✓ *Employee Training and Awareness*

Implementation Considerations



Total prohibition on use of generative AI

Little or no restriction on use of generative AI

Range of options based on the specific use cases and risk tolerances of the organization:

- Limit use to only internal research projects, no use for other business functions
- Limit use to only internal business functions, but no use in software development, content generation or other customer facing applications
- Allow for use in software development, but with heightened code review standards
- Allow for use in product / service without passing user personal data

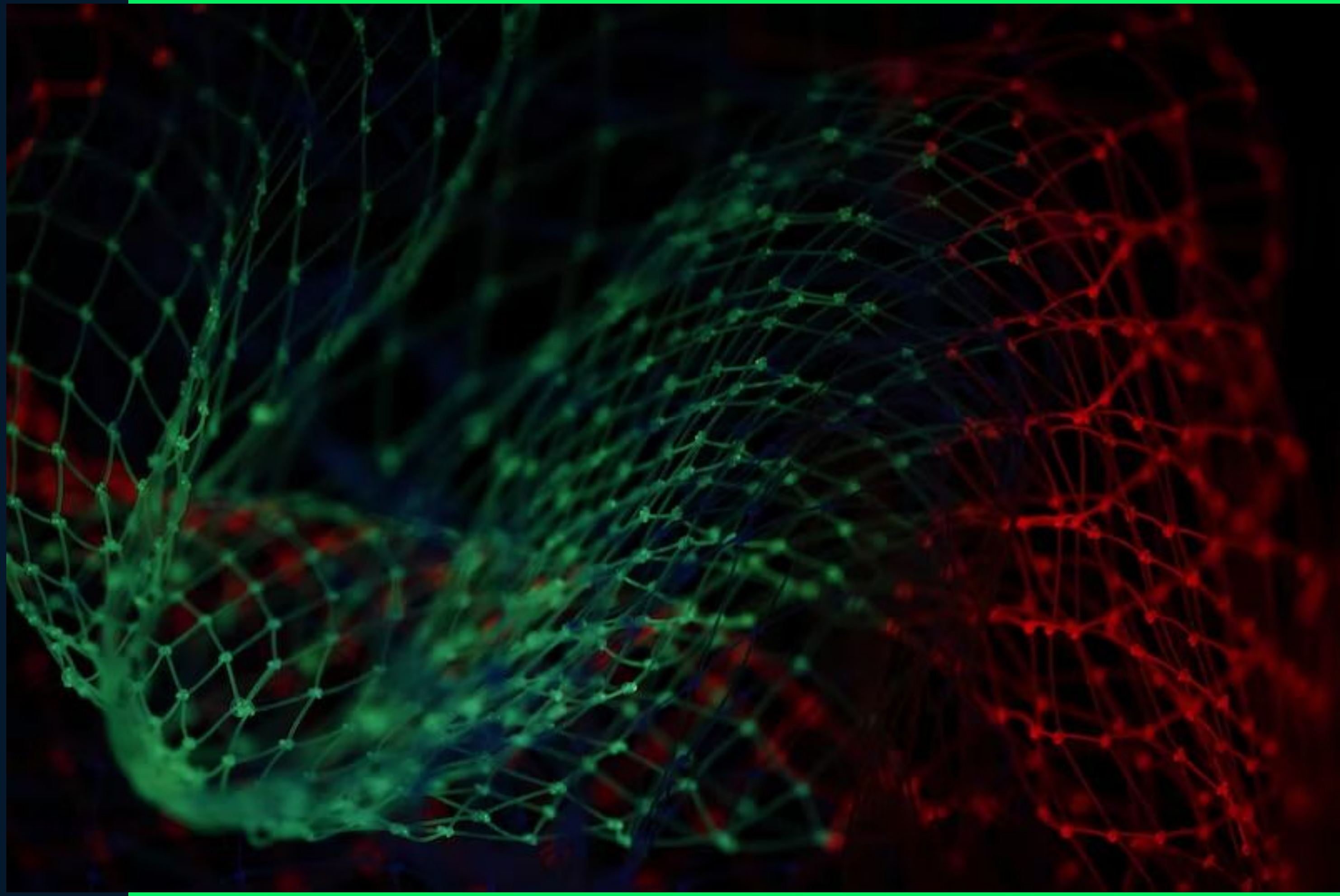
Incorporating AI in Services

1 Changes to Terms of Service will depend on use

- ✓ *For limited use that does not pass personal information, you may conclude that no changes are necessary*
- ✓ *But as more personal information is passed (for example in the context of personalized recommendations) you may need to update terms of service, privacy policies and DPAs*

2 Changes to Product / Service

- ✓ *Generally required (or strongly recommended) that users be informed about the use of AI systems in providing services*



5

Who to involve

Key stakeholders

Data teams

Engineering

Legal

Compliance

Privacy

Security

Business

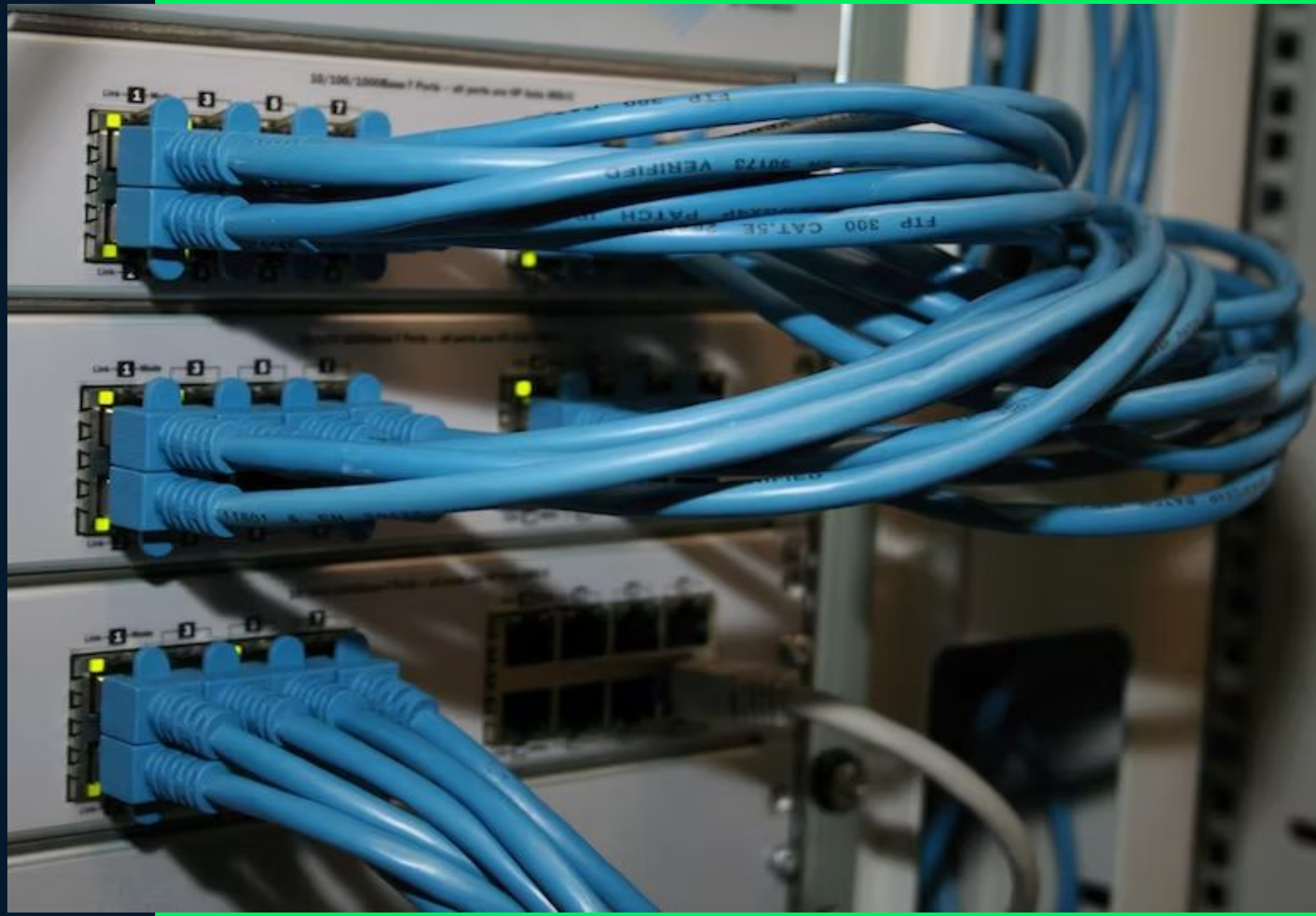
6

Additional Considerations

IP Considerations

Copyright

- ✓ *Models are trained using large public data sets and the models currently do not provide source attribution for the output*
- ✓ *Difficult to evaluate whether the output constitutes an unauthorized reproduction of another's work (i.e. copyright infringement)*
- ✓ *Providers have granted users the right to use content created by the model, those may not be sufficient to claim copyright protection over the content*



Q&A

LEARNING WITH YOUR TEAM?
CHECK OUT DATACAMP FOR BUSINESS

Thank you

clear as data