the global voice of the legal profession®

A conference co-presented by the IBA Intellectual Property and Entertainment Law Committee, the IBA Technology Law Committee and the IBA Healthcare and Life Sciences Law Committee

9th Annual World Life Sciences Conference

1–2 June 2023, The Kimpton Monaco Hotel, Washington, DC

Follow us @IBAevents

Wifi Network: Kimpton_meeting

Password: fast

Plenary session two – From primary to secondary use of health personal data, from open data to Intellectual property investment protection: is privacy opposed to data valuation?

Fabio Alonso Vieira
Kestener & Vieira Advogados

Cécile Théard-Jallu
De Gaulle Fleurance

Scott Jones
Johnson & Johnson

Kim Le
Debevoise & Plimpton

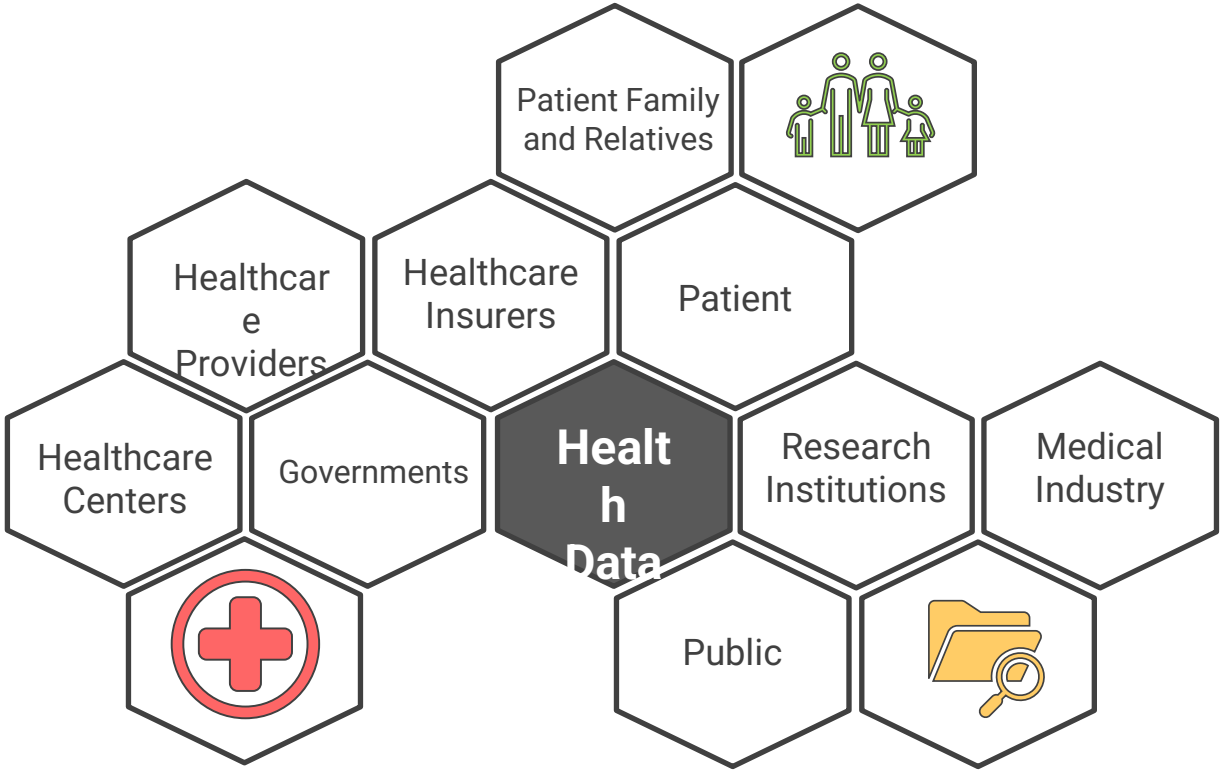
Samuli Simojoki
Borenius Attorneys Ltd

KESTENER VIEIRA
ADVOGADOS

HEALTH DATA: PRIMARY AND SECONDARY USE

IBA 9th Annual World Life Sciences Conference

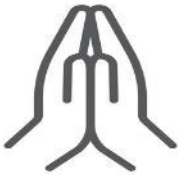
Health Data: Stakeholders and Interests



Health Data: Governance and Rulemaking

Constitutional Rights and Freedoms

Ethics



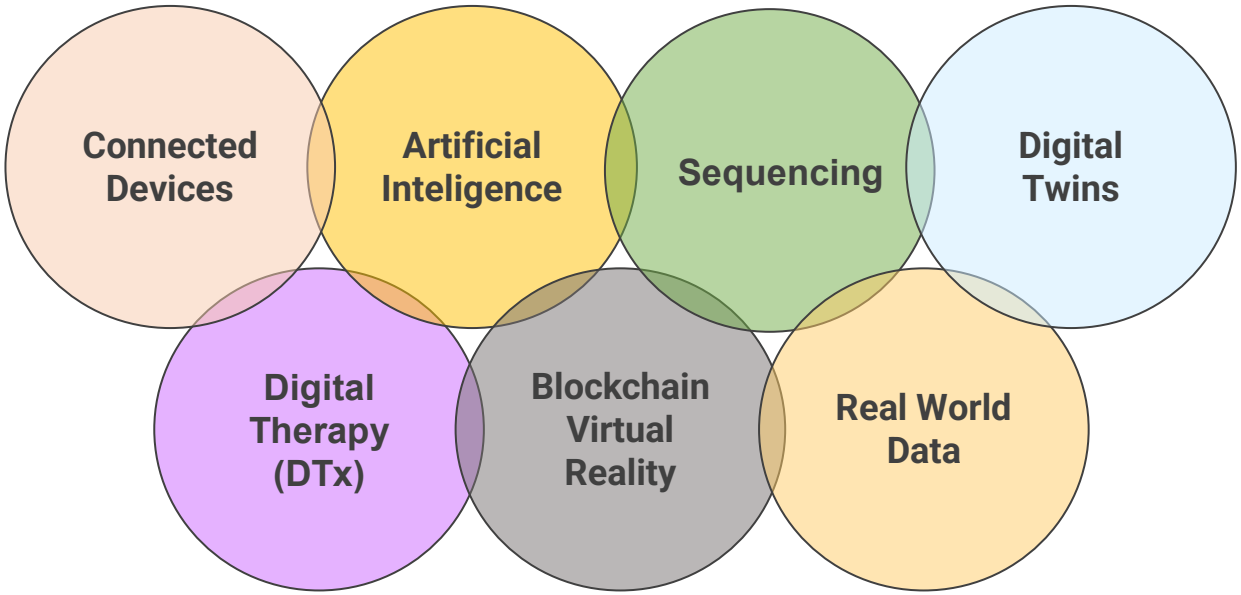
Religious Values

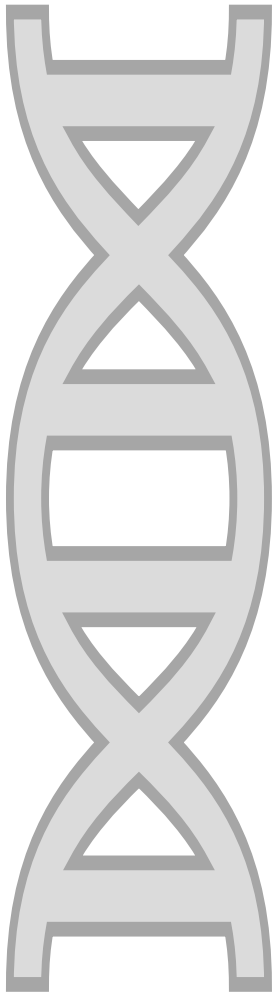
Laws / Regulations

Market Consent

Soft Law / Private Associations

Technological Advances in the Health Space





Speakers

Moderators:

Fabio Alonso Vieira I Kestener & Vieira, São Paulo
Cécile Théard-Jallu I De Gaulle Fleurance, Paris; Co-Chair, IBA Healthcare and Life Sciences Law Committee

Speakers:

Scott Jones I Johnson & Johnson, Washington, DC
Kim Le I Debevoise & Plimpton, San Francisco, California
Samuli Simojoki I Borenius Attorneys, Helsink

KESTENER VIEIRA
ADVOGADOS

Rua Fidêncio Ramos, 195, 8° andar
Conj. 81-83, 04551-010, São Paulo SP

+55 (11) 3149 6100

WWW.KVLAW.COM.BR

Compliant Use of Health Data: A Global Corporate Approach

Scott Jones
Senior Counsel
Johnson & Johnson
1 June 2023

Shaping health and well-being since 1886

We are a “**keep you healthy your whole life**” company.

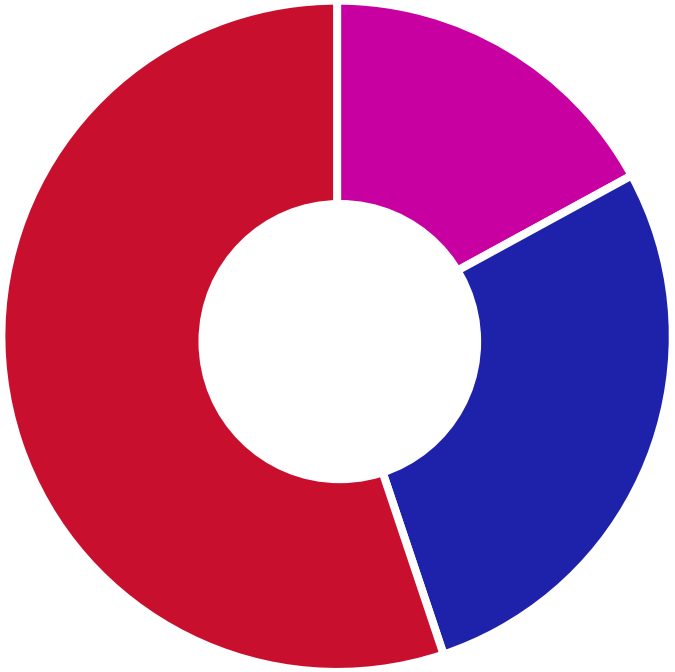
Johnson & Johnson

Our three business segments

*2022 Annual Report

Major segments

- Pharmaceutical
- MedTech
- Consumer Health



152,700 employees worldwide

Johnson & Johnson

Global Data Protection Laws and Regulations

U.S. Laws and Regulations

Our Data Privacy and Security Program

Federal

- HIPAA
- FTC Act
- FTC Health Breach Notification Rule
- Privacy Act of 1974
- FDA Quality Systems Regulation
- FD&C Act (including 2023 Consolidated Appropriations Act)
- COPPA
- CAN-SPAM
- Telephone Consumer Protection Act
- FCC marketing rules
- Electronic Communications Privacy Act / Wiretap Act
- Video Privacy Protection Act
- Computer Fraud and Abuse Act
- Defend Trade Secrets Act
- Sarbanes Oxley
- SEC Disclosure Rules

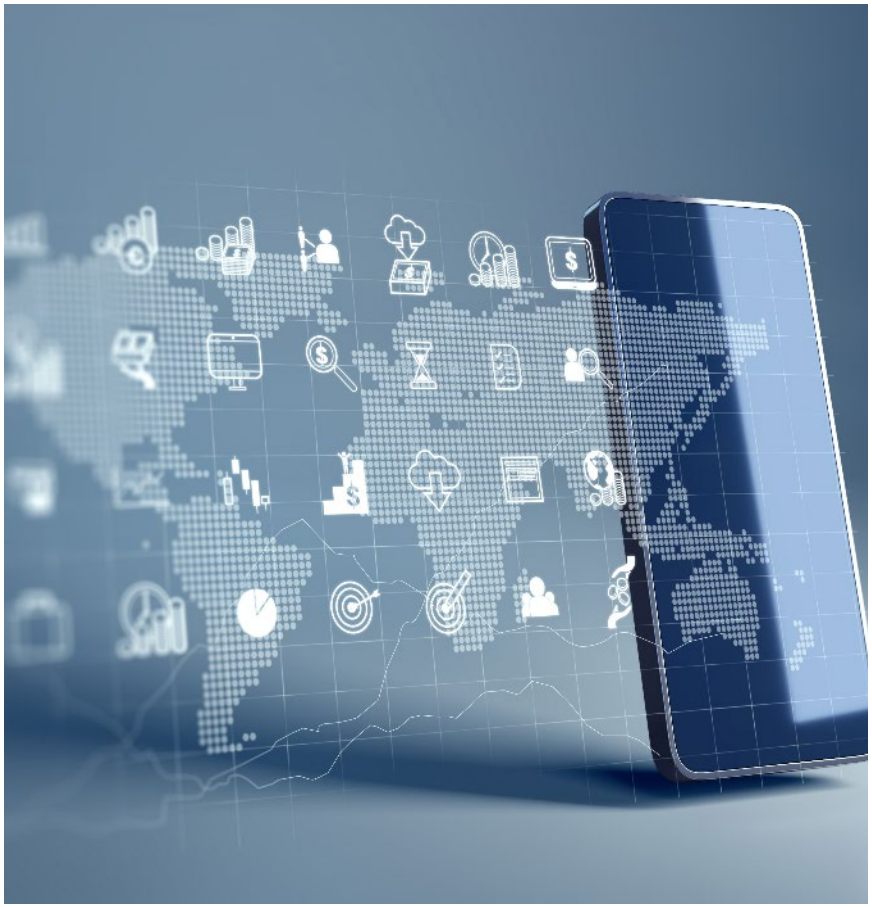
State

- Consumer Privacy Omnibus laws
- Data breach notification laws
- Health information privacy laws
- Biometric laws
- Wiretap laws
- Mini-FTC and TCPA Acts

Johnson & Johnson

Non-U.S. Laws and Regulations

Our Data Privacy and Security Program



- EU Charter of Fundamental Rights
- GDPR / EU member state laws
- ePrivacy Directive
- NIS Directive (2.0 forthcoming)
- Cybersecurity Resilience Act
- UK GDPR
- FADP (Switzerland)
- LGPD (Brazil)
- PIPEDA & provincial laws (Canada)
- PIPL, CSL, DSL (China)
- IT Act & SPDI Rules (India)
- APPI (Japan)
- PIPA (South Korea)
- POPIA (South Africa)

Lead in Accountability & Innovation

Our Data Privacy and Security Program

Principle-based Global Compliance

Our Data Privacy and Security Program

- Our Credo
- Codes of Conduct
- Privacy Compliance Framework


Johnson & Johnson

International Bar Association
9th World Life Sciences Law Conference

Washington DC, USA

June 1 & 2, 2023

Protection & sharing of health data
Under EU law

Cécile *Théard-Jallu*, Partner

DE GAULLE FLEURANCE

LEGAL STEP TO CHANGE

EU RULES ON THE PROTECTION AND SHARING OF DATA

National Public Health Rules

GDPR & National Personal Data Protection Rules

FREE FLOW OF NON PERSONAL DATA ACT

DATA GOVERNANCE ACT

EU & National Intellectual Property Rules

DATA ACT

EU & National Open Data Rules

EHDS ACT (Tehdas)

Othe Europ Data Spac

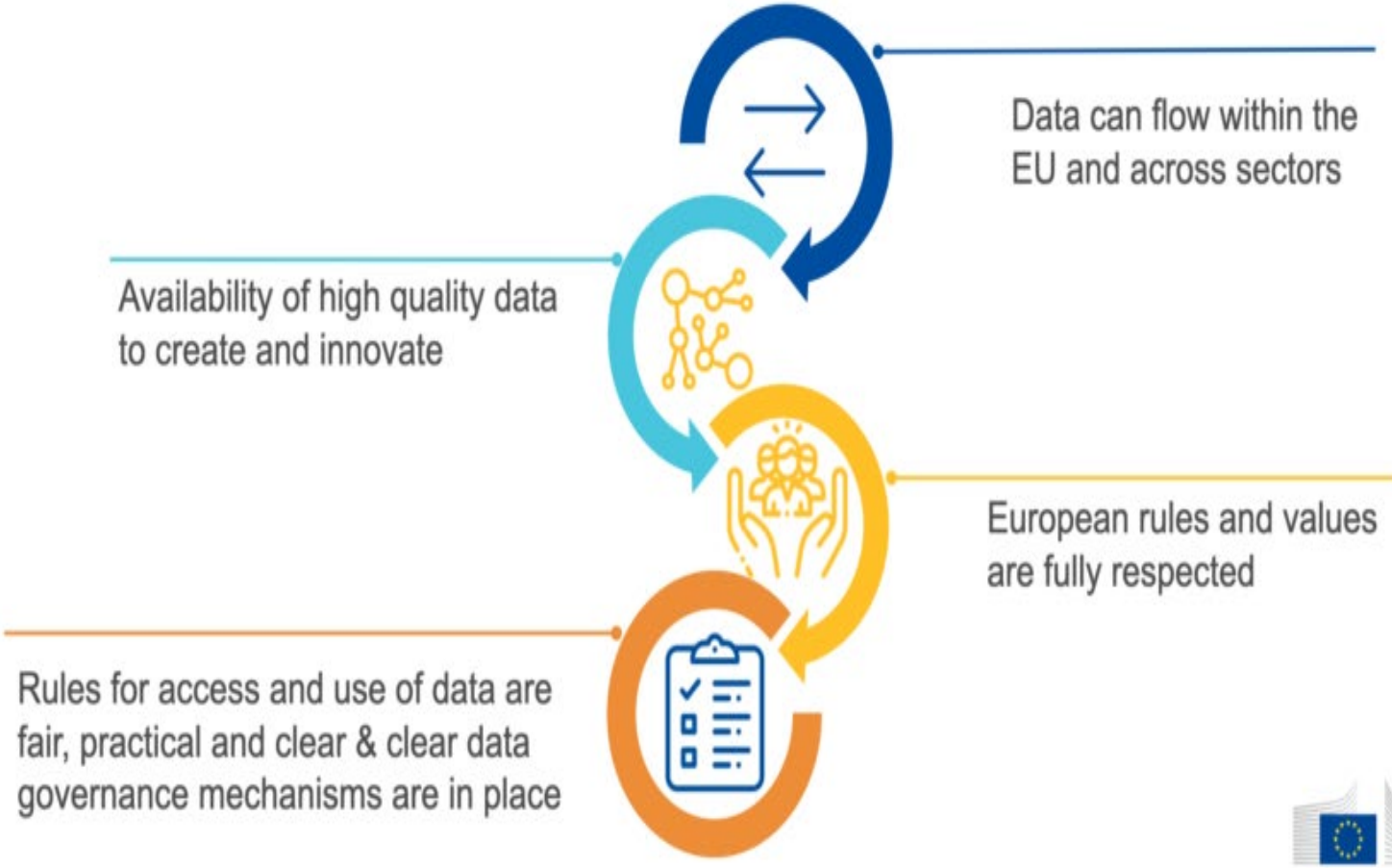
EU & National Cybersecurity rules

AI ACT & Human Oversight

DE GAUL FLEURAN

European Strategy for Data

A common European data space, a single market for data



Source: https://dataspaces.info/common-european-data-spaces/#page-content

Cheaper prices for aftermarket services and reparation of their **connected objects**.

A factory robot breaks down.

TODAY	TOMORROW
Only the manufacturer can access the data, leaving no alternative for the company but to call them for repairing.	*The user could request that a repair service that may be cheaper also gets access to the data.*

New opportunities to use services relying on access to this data.

A farmer has equipment from different manufacturers (tractor, automatic irrigation system).

He cannot outsource the data analytics of its different equipment, the data is locked with each manufacturer.	*He could receive customised advices from a company gathering data from the different equipment.*

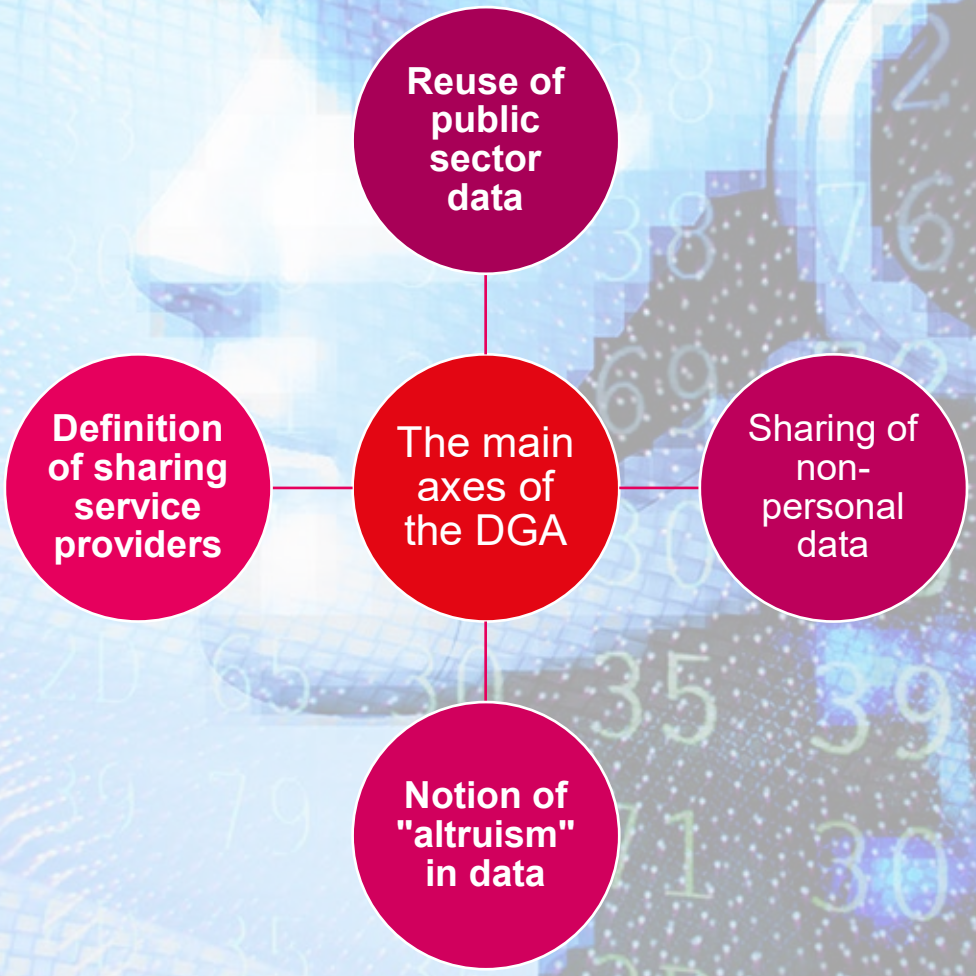
Better access to data collected or produced by a device.

A bar owner wants to serve better coffee, and the coffeemaker company wants to improve its product.

Only the company can access the data produced by the machine to design the next generation of coffeemakers but the bar owner cannot access information such as the quantity and temperature of water or coffee strength.	*The Data Act clarifies that both parties can access all data collected by the machine.*

Source: https://www.eu-data-act.com/

Data Governance Act (DGA) – 30 May 2022 / Sept 2023



Draft EU Data Act (DA) (23 February 2022)

- **1. Strengthening users' rights**
  - Obligation for data holders to make the data generated by them on users available to users free of charge
- **2. New data sharing requirements from companies to governments**
  - In certain exceptional circumstances (e.g.: a health crisis or natural disaster) companies may be required to share their data with public institutions, including governments, free of charge
  - Compensation may be requested by the data holder if it is requested in a preventive manner
- **3. Supporting SMEs in B2B data transfers**
  - EU Commission's target: unfair contractual clauses, i.e., those imposed unilaterally on an SME by a more powerful party in a data sharing contract between companies
- **4. Easier switching between cloud and edge services**
  - Minimum rules to enable switching between cloud and edge services
    - new contractual, commercial and technical requirements
  - Obligation to set various measures to prevent governments outside the EU from illegally accessing data stored in EU clouds
- **5. An horizontal basis for future data spaces**
  - Sectoral acts destined to supplement the Data Act
  - Beginning by the health data space, due to be presented in April 2022?

Future European Health Data Space (2 May 2022)

Why?

- **To regulate the reuse of health data for purposes other than initial care**
- **Value of this activity according to the EU Commission:**
  - €25 billion today
  - Expected €50 billion in 2032

What to expect about the coming EU Health Data Space Act?

- **First sectoral Act combined with DGA + DA**
- **Requirements of cross frontier data quality standards & interoperability and pan European infrastructure**
- **Improve efficiency in care and scientific research, towards a "EU data market"**

=> "Free the health data market"

- **What about individuals' rights on 'primary' use and secondary use by design?**
- **What will be the scope and conditions of permitted 'Secondary use'? Which secondary use will be forbidden?**

- **Individuals' rights on 'primary' use**
  - Individuals should have the right to access a minimum set of 'primary' health data, including vaccination, electronic prescriptions, images, laboratory results, discharge reports, and others – using a free of charge access service
  - Individuals will also have the right to restrict access to such data or share it with third parties free of charge

- **'Secondary use' for personalized medicines**
  - Secondary use includes health records, social data, administrative data, genetic and genomic data, public registries, clinical studies, research questionnaires, and biomedical data such as biobanks
  - The list of **allowed uses** includes informing regulatory decisions and supporting public authorities in carrying out their tasks, as well as in education, scientific research, developing innovative solutions for public interests, and training algorithms with medical applications
  - Some purposes to be explicitly **forbidden**, such as informing decisions against individuals with legal effects, including insurance premiums, commercial advertising, and selling data to third parties

What's next?

- EHDS Act still on its legislative way
- Exchanges with data protection authorities
- Several articles yet to be specified through secondary acts (delegated or implementing acts)
- What about the EHDS Governance?" Establishment of a *"European Digital and Health Data Committee*
- *Source:* https://www.euractiv.fr/section/economie/news/leak-lespace-europeen-des-donnees-de-sante-pour-liberer-les-donnees-de-sante/

Draft European Health Data Space – 3 May 2022

Objectives of the Proposal regarding health personal data

- supporting individuals to take **control of their own health data**
- supporting the **use of health data for better healthcare delivery, better research, innovation and policy making**
- enabling the EU to make **full use of the potential offered by a safe and secure exchange, use and reuse of health data** within the EU

Main provisions of the Proposal related to data protection of the health data

- The Proposal is subject to the GDPR and EU Data Protection Regulation (EUDPR)
- “Add-ons” on the rights of data subjects regarding their health data
- Implementation of a EU platform “MyHealth@EU » for the management of health data at EU level
- Dedicated framework on the processing of health data for the two describe uses of health data (**primary and secondary uses**)

LEGAL STEP TO CHANGE

Thanks !

Cécile Théard-Jallu

Partner, De Gaule Fleurance

Mobile: + 33 6 07 26 93 43

E-mail : ctheardjallu@dgfla.com

9, rue Boissy d'Anglas, 75008 Paris - France - Tél. : +33 (0)1 56 64 00 00 Fax : +33 (0)1 56 64 00 01
222, avenue Louise, 1050 Bruxelles - Belgique - Tél. : +32 (0)2 644 01 64 Fax : +32 (0)2 644 31 16

contact@dgfla.com - **www.degaullefleurance.com**

DE GAULLE FLEURANCE

BORENIUS

IBA WORLD LIFE SCIENCES CONFERENCE WASHINGTON

SECONDARY USE OF HEALTH AND SOCIAL DATA - THE FINNISH EXPERIENCE

SAMULI SIMOJOKI

BORENIUS ATTORNEYS

BORENIUS

ACT ON THE SECONDARY USE OF HEALTH AND SOCIAL DATA

- Passed into law 2019
- Purpose: enable use of health and social data held in public registries in Finland for
  - Planning and reporting duties of authority
  - Education
  - Statistics
  - Scientific research

- Legislative process involved privacy related bumps in the parliament

AUTHORITIES WHOSE DATA AVAILABLE

- Data saved in central healthcare database Kanta
- Digital and Population Data Agency
- Finnish Center for Pensions
- Finnish institute for Health and Welfare
- Finnish institute for Occupational Health
- Finnish Medicines Agency Fimea
- National Supervisory Authority for Health Valvira
- Public and private service providers of social welfare and health care
- Social Insurance Institution of Finland
- Statistics Finland
- Regional state administrative agencies

PROCESS FOR USE OF SECONDARY DATA

- Findata: a new organisation managing the secondary use
- Applications for use of data to (i) data controller or (ii) to Findata, depending on situation
- Detailed regulations on access rules and process in relation to use of data
- Data provided to applicant in pseudonym form
- Processing only in trusted research environment managed by Findata or certified data system
- Assumption: processing of personal data based on public interest. Data subjects have rights under the GDPR
- Anonymization only by Findata!
  - → if results of the research published, Findata needs to be involved

DATA REQUESTS

- Wide variety of methods to select data (including data on relatives and data on control groups)
- Examples:
  - Live births and stillbirths of foetuses with a birth weight of at least 500 g or with a gestational age of at least 22 weeks. Mothers of the abovementioned children.
  - Patients in inpatient care and periods of care in Finnish health care in 2015.
  - Recipients of social assistance in Southwest Finland in 2014

PROJECTS USING THE DATA

2022: 85 data sets delivered

Examples of projects:

14.12.2022

StellarQ Oy

30.11.2022

MedEngine Oy

05.05.2023

Karolinska Institutet

Antibiotics, maternal metabolic and perinatal complications and subsequent risk for psychiatric disorders, diabetes and obesity in childhood and adolescence

Issued: 05.05.2023
Valid until: 31.12.2027
Purpose of data use: Tieteellinen tutkimus

#17192991

BORENIUS

OUTCOME

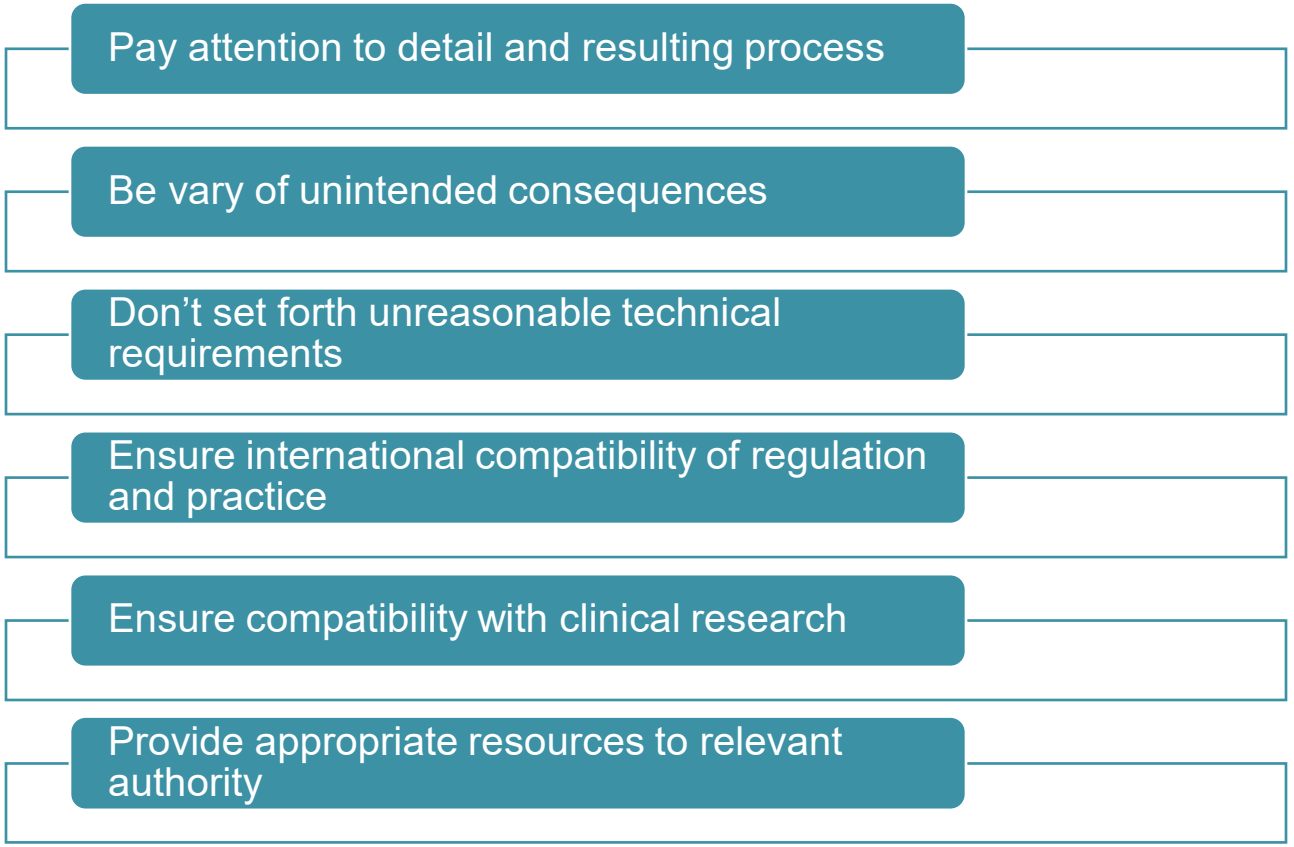
UNINTENDED CONSEQUENCES FOR UNIVERSITIES AND OTHER PUBLIC AUTHORITIES

- Almost disaster for research at university hospitals
  - Restrictions on use of university's own data for secondary use
  - Significant restrictions on ability to of university hospitals to submit data to international research databases
    - Requirements for trusted research environments
    - Data permit must specify organizations and persons accessing the data
  - Findata's anonymization monopoly: university hospitals not able to share anonymous data without overly burdensome and costly process

MODERATE – BUT NOT IMMEDIATE – SUCCESS FOR PRIVATE ORGANIZATIONS

- Earlier no access to data for secondary use
  - → now in theory extensive access
- Problems:
  - Narrow definition of research purpose (or interpretation by authorities?)
  - Slow and complicated process
  - Limited usability of trusted research environments

LESSONS LEARNED



SAMULI SIMOJOKI

Partner

Mob. +358 40 571 3303
Samuli.simojoki@borenius.com

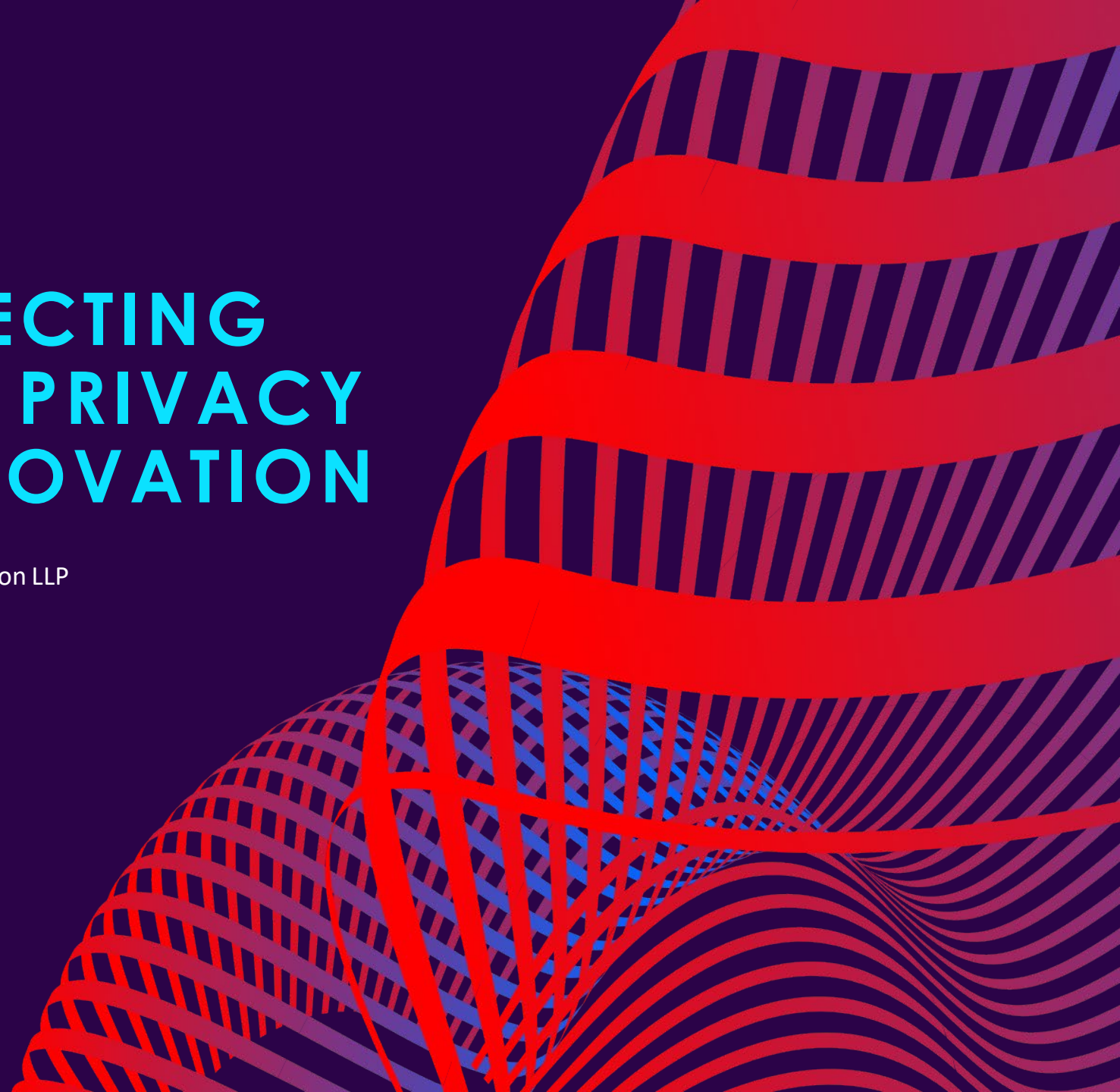
BORENIUS

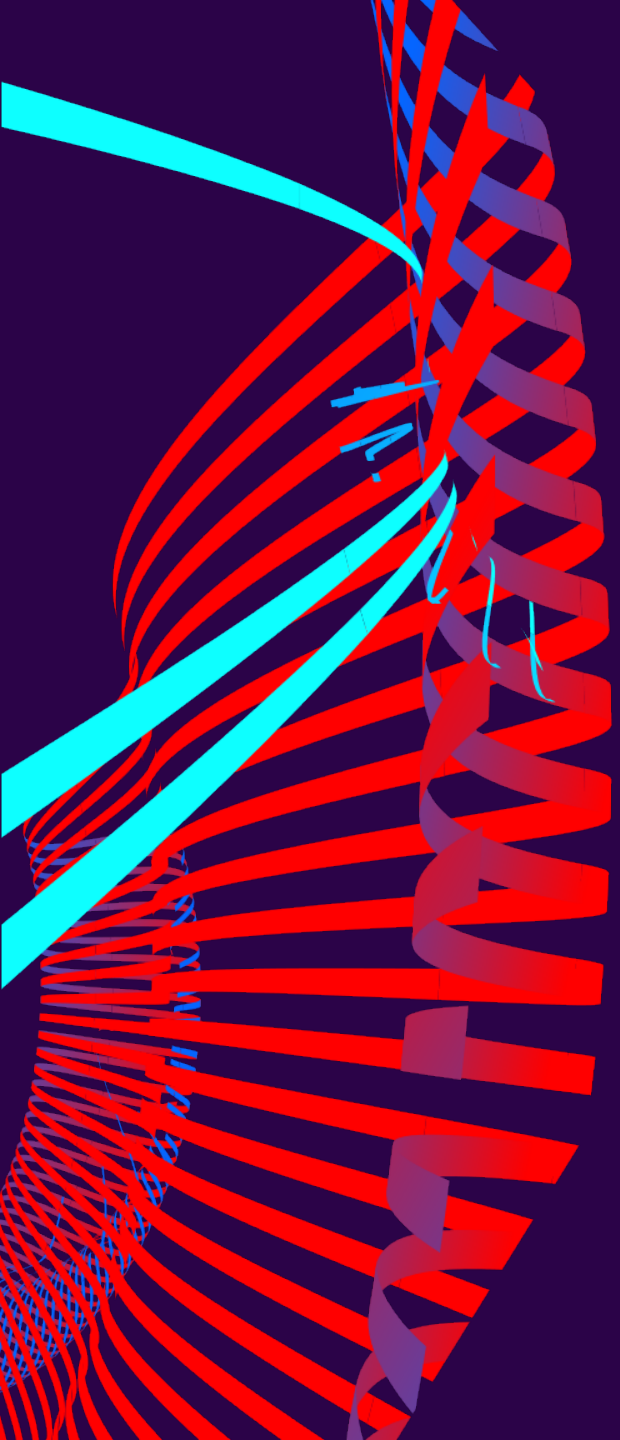
BORENIUS ATTORNEYS LTD, Eteläesplanadi 2, FI-00130 HELSINKI, FINLAND

Office: +358 20 713 33 info@borenius.com www.borenius.com

PROTECTING DATA PRIVACY & INNOVATION

Kim T. Le
Debevoise & Plimpton LLP





INTRODUCTION

PATCHWORK APPROACH

The United States continues to take a piecemeal, sectoral approach to privacy regulation. Though a unified national data privacy framework would do much protect consumer data, promote transparency, and provide regulatory certainty in the marketplace, attempts to create broader privacy protection at the federal level have been to date unsuccessful. Congress made bipartisan progress on enacting comprehensive federal privacy legislation last year, advancing the proposed American Data Privacy and Protection Act (ADPPA) to the cusp of a U.S. House floor vote. These efforts have been stymied by myriad issues—particularly state preemption concerns.

MULTIPLE REGIMES

FTC

The Federal Trade Commission has operated as a "de facto" privacy regulator. Section 5 of the FTC Act prohibits "unfair and deceptive acts or practices in or affecting commerce."

HIPAA

Strict limitations on the use and disclosure of "Protected Health Information" (PHI) by "Covered Entities" and their "Business Associates." Broad exceptions for research, de-identified data.

State Laws

To date, California, Colorado, Connecticut, Utah, Washington and Virginia have enacted (and Indiana, Montana, and Tennessee have passed, but not yet signed) comprehensive data privacy laws.

ADPPA

Lawmakers are signaling a continuing appetite for a national privacy framework. The March Congressional hearing saw support for the proposed ADPPA as a solution to current regulatory shortcomings.

REEVALUATING REIMAGINING REINVENTING HEALTHCARE

The global pandemic has irrevocably altered our approach to healthcare innovation and advancement. Data has certainly played a key role in enabling cross-border, as well as cross-sector, collaboration to optimize public health responsiveness. More than even this, data will be the key to the optimization of care delivery and health outcomes—without it, we risk being ill-equipped to meet the needs of a growing, ageing population with increasingly-complex chronic disease management demands.

HOW DATA FUELS INNOVATION

Research

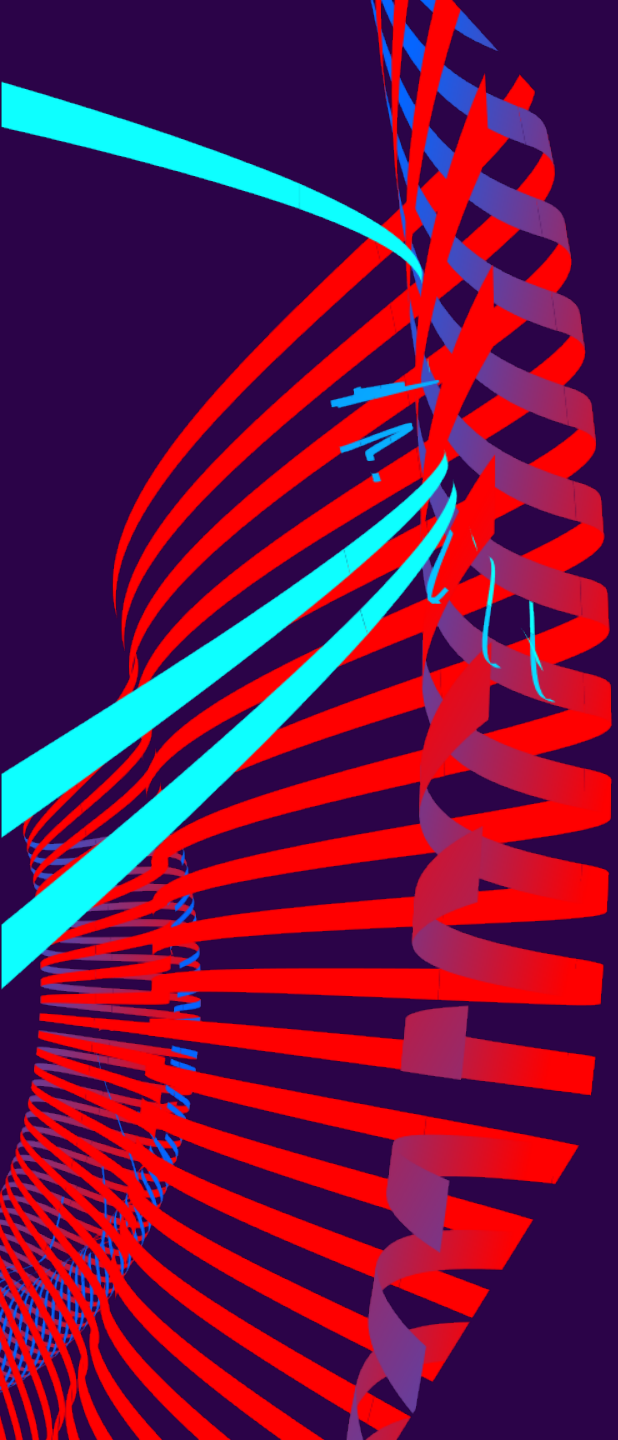
- Expedites drug and device development
- Improves research integrity
- Allows decentralization
- Facilitate analytics and predictive modelling

Patients

- Personalized interventions and advanced diagnostics
- Fuels remote monitoring, care
- Expands and improves access, particularly for marginalized communities

Health Systems

- Reduces healthcare costs
- Enables population health management and care coordination across the patient care spectrum
- Optimizes clinical outcomes



SPOTLIGHT: FTC ACTIVITY

DECEPTIVE PRACTICES UNDER THE FTC ACT

A practice is "deceptive" where it involves a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. For example, a company's consumer-facing privacy policy may state that it does something with regard to personal information (e.g., "we encrypt your data in transit and at rest") that, in practice, it does not.

UNFAIR PRACTICES UNDER THE FTC ACT

An act or practice is "unfair" if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. This has long-been interpreted as establishing a baseline "reasonableness" standard for companies with respect to their information security program design and their adoption of practices to appropriately protect personal information.

CASE STUDY: LABMD

- In 2010, the FTC was notified that files belonging to LabMD may have inadvertently been made publicly available through an employee's use of LimeWire—a peer-to-peer file-sharing program—exposing the personal information of 9,000+ consumers to a high risk of unauthorized access.
- The FTC alleged LabMD failed to implement "reasonable" security practices such as intrusion detection systems, file integrity monitoring, firewall traffic monitoring, security training for employees. It also alleged a failure of risk-reducing data minimization practices because the company had been storing consumer information longer than necessary. LabMD appealed the FTC's findings, arguing the allegation was too vague as to be enforced.
- In 2018, a federal court of appeals sided with LabMD, ruling the term "reasonable" was "devoid of any meaningful standard."
- In practical terms, the LabMD case represented a major inflection point for the FTC's enforcement approach. Post-LabMD, FTC began (i) alleging with granularity how respondents violated federal law and (ii) drafting settlements containing more specific remedial measures—e.g., restrict inbound IP connections, require authentication, limit access by function, implement MFA, perform vulnerability testing at least once per quarter.

HEALTH BREACH NOTIFICATION RULE

Generally requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information (or a breach of same by a service provider).

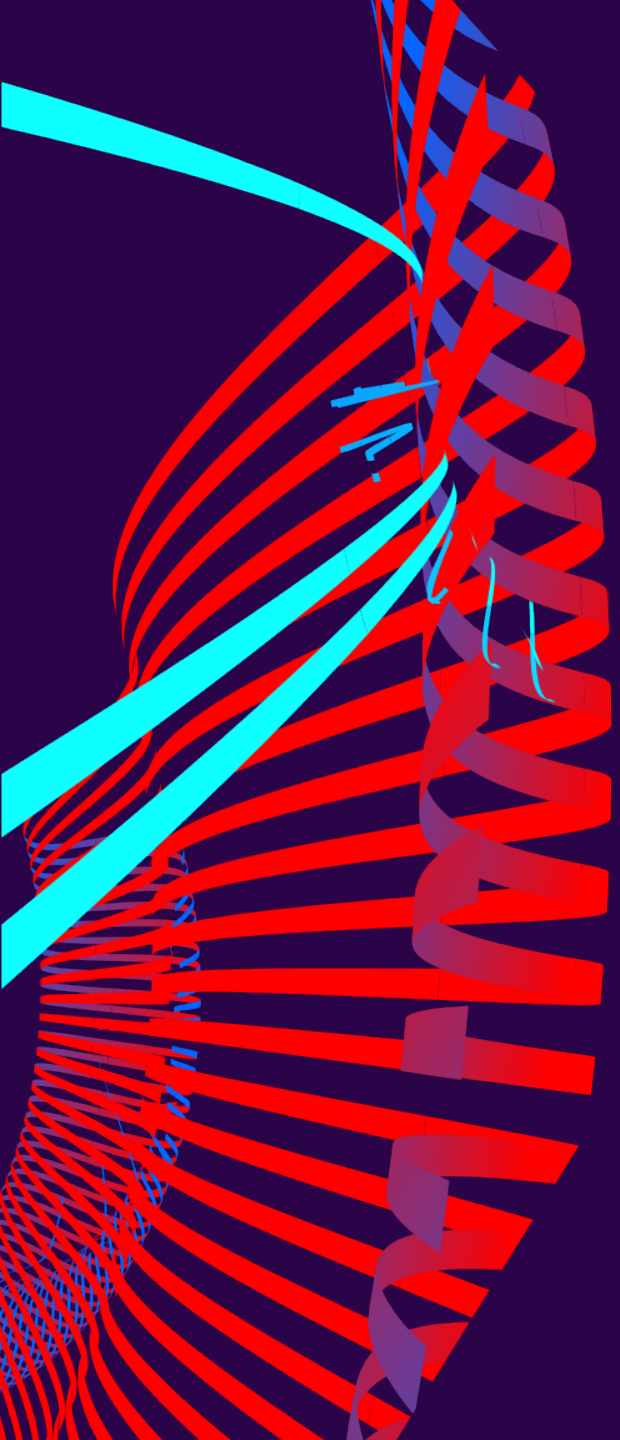
In 2021, the commission issued a policy statement that clarified the Health Breach Notification Rule applies to most health apps and similar technologies.

THE FTC POST-DOBBS

In July 2022, President Biden signed an Executive Order—"Protecting Access to Reproductive Health Care Services"—in response to the Supreme Court's overturning of Roe v. Wade. Part of the Order directs the FTC to confront violative practices related to protecting consumers' privacy when seeking information about and provision of reproductive health services. The FTC issued a statement that it considered location and health information, particularly regarding personal reproductive matters, to be among the most sensitive information deserving of enhanced privacy and security protections.

CASE STUDY: PREMOM

- On May 17, 2023, the FTC announced a proposed settlement agreement (in the form of a stipulated order) with Easy Healthcare Corporation, which operates the "Premom" fertility tracking app.
- The FTC alleges Premom (i) made deceptive statements in its privacy policy—including statements that it would only collect and use nonidentifiable user information—to consumers, and (ii) failed to provide notice to users when it shared their health information without their consent.
- This is the second enforcement action that the FTC has brought under its broad interpretation of the Health Breach Notification Rule, following its first enforcement action in February against GoodRx.
- The proximity between these two enforcement actions—combined with the FTC's Notice of Proposed Rulemaking (NPR) modifying the Health Breach Notification Rule last week—indicates the FTC's continued interest in, and ever-broadening regulation of, digital health privacy.
- The NPR's most significant proposed change is to clarify that a security breach includes any unauthorized acquisition of identifiable health information that occurs as a result of a disclosure. Currently, the language of the Rule can be interpreted to apply only to malevolent breaches.



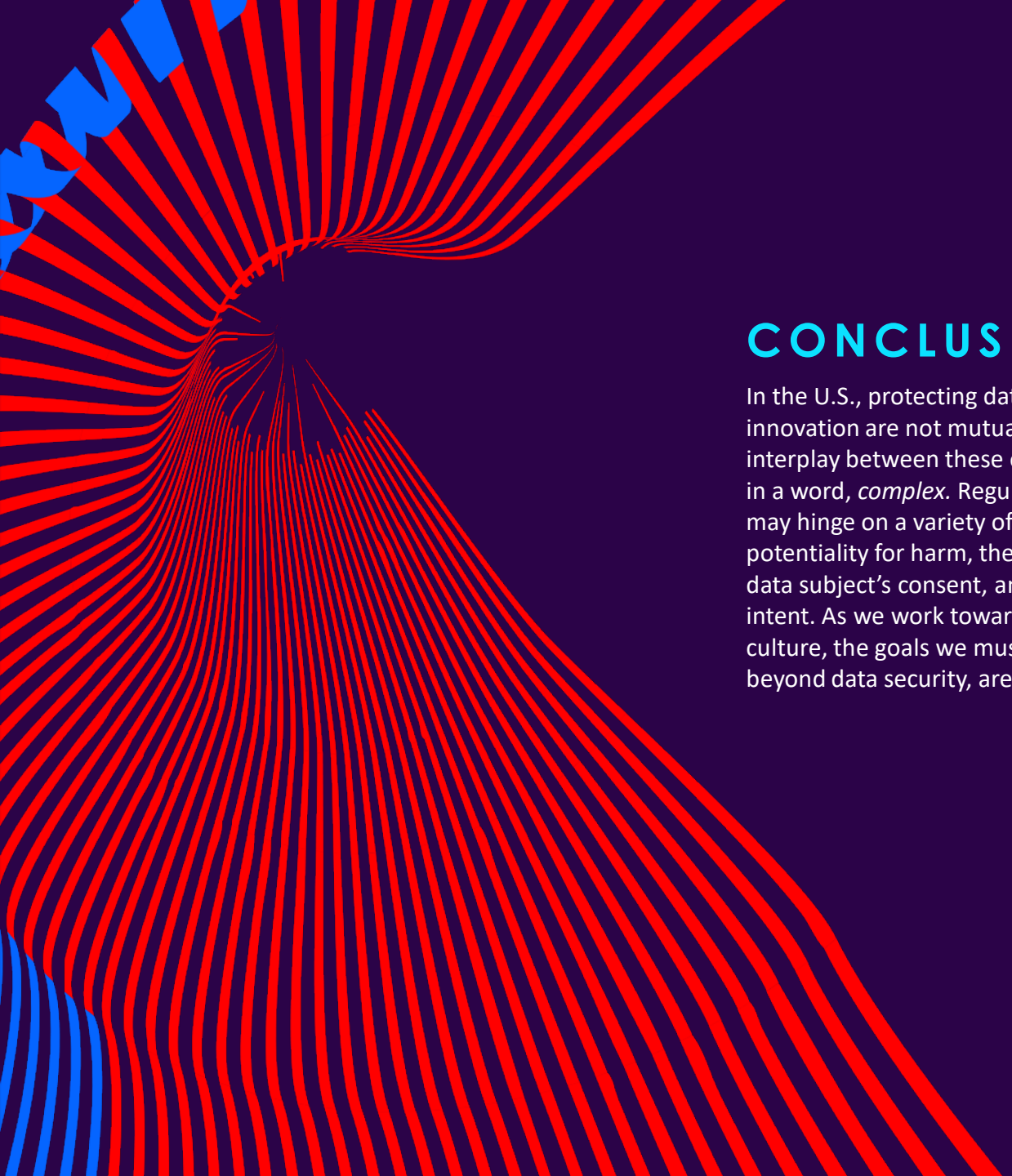
SPOTLIGHT: ADPPA REDUX

PUBLIC HEALTH EXCEPTION

The ADPAA is top of mind for a broad swathe of lawmakers and, if enacted, would be add to the FTC's arsenal. The ADPPA, as currently drafted, excludes data protected by HIPAA—which contains a broad exception for disclosures of personal information made in the interest of public health and safety. In today's world, however, health data doesn't just reside with Covered Entities and their Business Associates. Because the ADPPA does not appear to contemplate a public health exception, it may, inadvertently, hinder progress on predictive analytics and outbreak response.

STATE LAW PREEMPTION

State law preemption is a major pain point on the road to enacting a unified national data privacy framework. In particular, the state of California has been vociferous in its opposition, calling on Congress to "set the floor and not the ceiling" in any federal privacy law, and to allow states to provide additional protections in response to an ever-changing technology landscape. If the ADPAA is to make any headway, we're likely to see express adoption of California's most stringent provisions—e.g., requiring explicit, opt-in consent from the consumer to use personal data in a "secondary" way.



CONCLUSION

In the U.S., protecting data privacy and fueling innovation are not mutually exclusive goals—but the interplay between these oft-competing interests is, in a word, *complex.* Regulation and enforcement may hinge on a variety of factors, including the potentiality for harm, the potentiality for good; the data subject's consent, and the data processor's intent. As we work towards an effective data-sharing culture, the goals we must keep top of mind, far beyond data security, are ethical in nature.

THANK YOU

Kim T. Le

+1 415.738.5706

kle@debevoise.com

www.debevoise.com