NGI POINTER WEBINAR

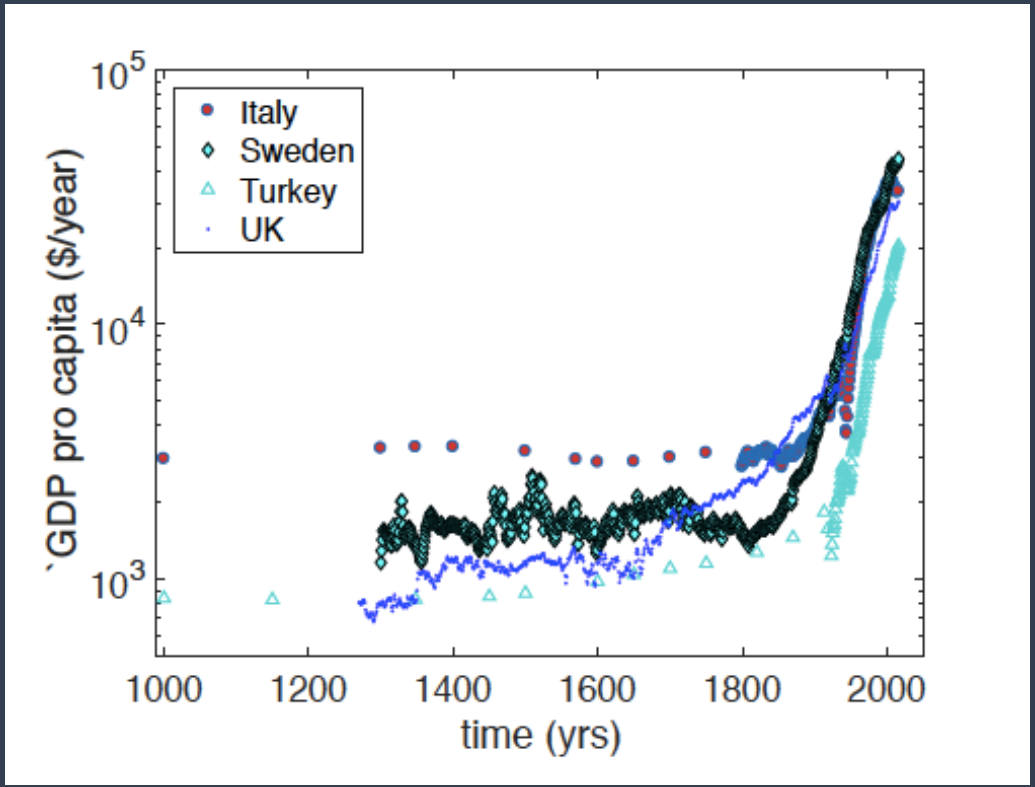
“Digital contact tracing & the future of privacy”

June 25th 2020

Manuela Battaglini Manrique de Lara
CEO - Transparent Internet
@manuelabat

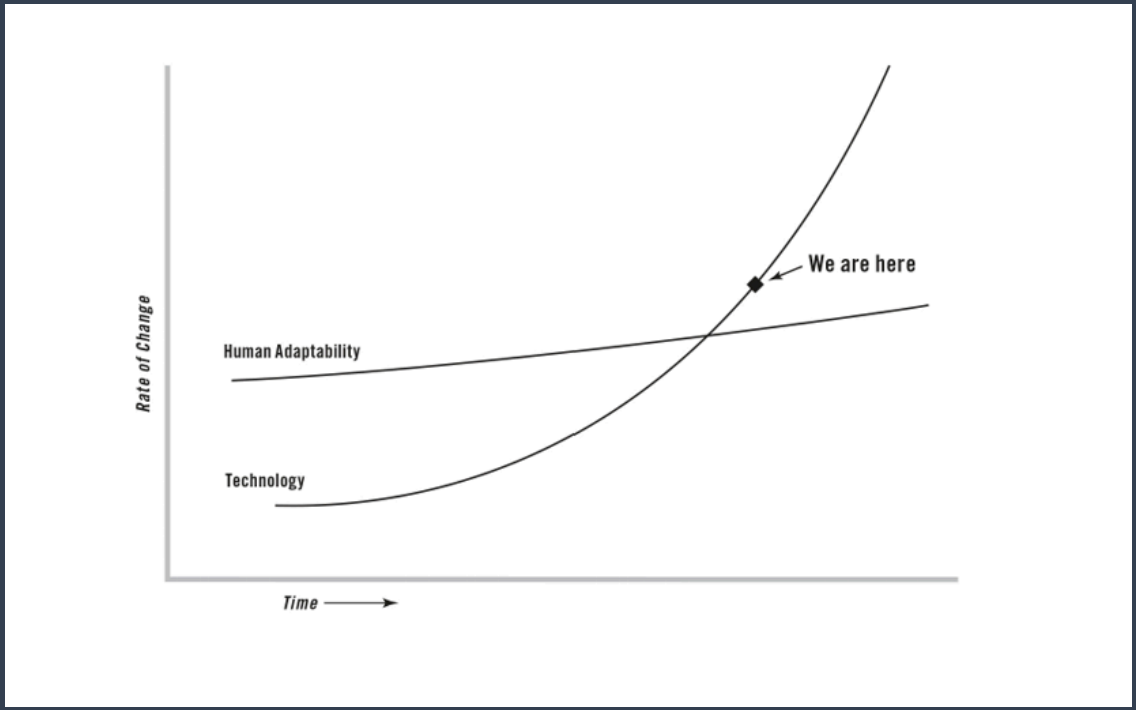
Mistrust of COVID-19 apps is just part of the normal process of adapting to a new technology.

Big picture: Evolution of human wealth in 1000 years



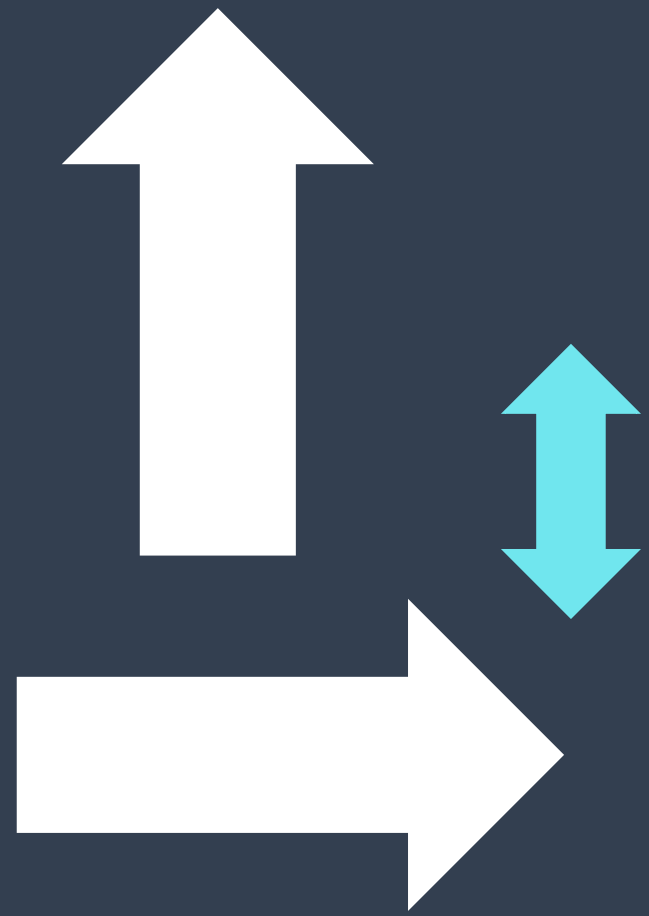
Source: Sibani & Rasmussen, Human wealth evolution: trends and fluctuations, 2020 (in review)
https://arxiv.org/pdf/2003.11502.pdf

Where are we now, and why?



Source. Friedman,T. L. (2016) 'Thank you for being late: An optimist's guide to thriving in the age of accelerations', Penguin Group, London, p. 32.

Consequences



PHYSICAL TECHNOLOGIES

Internet, Big Data, Artificial Intelligence/Machine Learning, Nano Technology, IoT, Robotics and Automation...

GROWING GAP

SOCIAL TECHNOLOGIES

Public Administration, Governments, Education, Culture, Institutions, Laws

Where are we now?

Ethical and social framework for COVID-19 apps

Same objective, different interests.

We need to strike a balance between:

1. **Global balance.** Governments - control of the pandemic.

2. **Local balance.** Citizens - feeling safe in all scenarios of their lives (family, leisure, social life, work...), and not being discriminated.

Ethical and social framework for COVID-19 apps

1. **The central issue: effectiveness in containing the spread.** Penetration of 60% of the population. In different countries it has not reached a penetration of more than 25%.

2. **The WHO** indicates its fear of discrimination,** threats and violence against users, or those who for various reasons cannot use the application.

*Ferretti, L. et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 368, no. 6491 (2020).
**https://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf

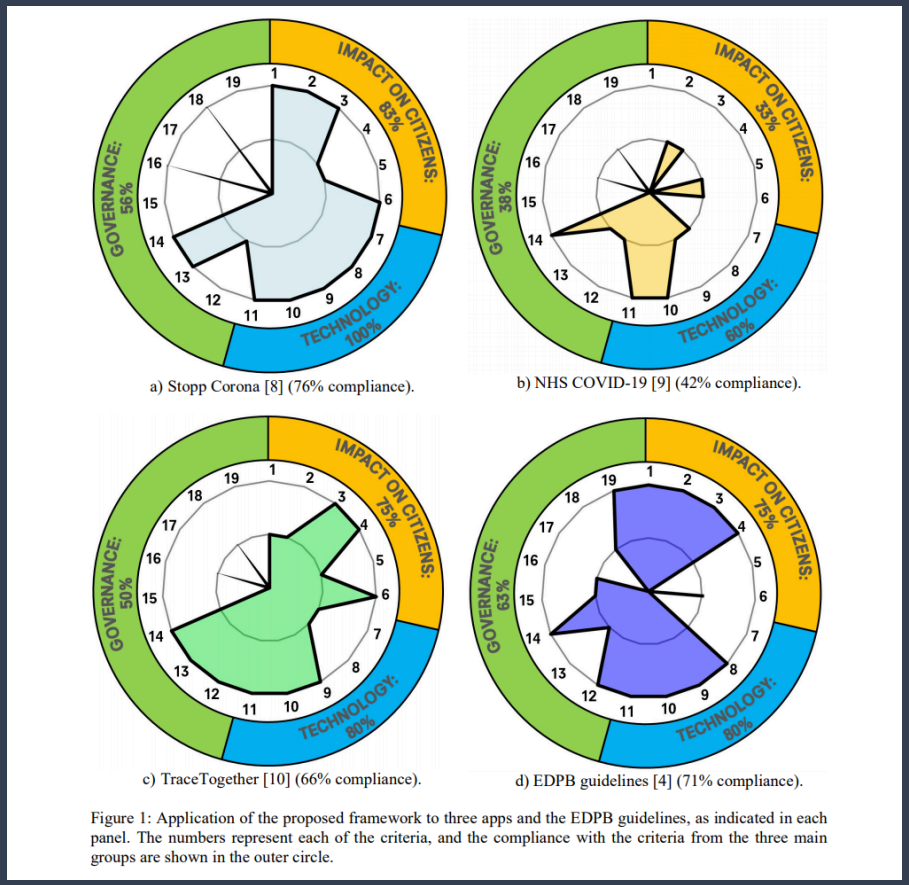
Ethical and social framework for COVID-19 apps

A. IMPACT ON CITIZENS

1. **Fundamental rights of individuals.** Rights to safety, health, non discrimination and freedom of association, among others.
2. **Privacy and data protection. DPIA.**
3. **Right to Transparency.**
4. **Avoiding stigmatization** due to suspicion of contagion.
5. **Accessibility.** Possibility to be used by all regardless of demographics, language, disability, digital literacy and financial accessibility.
6. **Education and tutorials.**

B. TECHNOLOGY.

7. Decentralised Protocol (DP-3T). Interoperability. Bluetooth.
8. Data management. Data protection and Privacy by design.
9. Security. User authentication to prevent risks such as access, modification, or disclosure of the data. Use unique and pseudo-random identifiers.



a) Stopp Corona [8] (76% compliance).
b) NHS COVID-19 [9] (42% compliance).
c) TraceTogether [10] (66% compliance).
d) EDPB guidelines [4] (71% compliance).

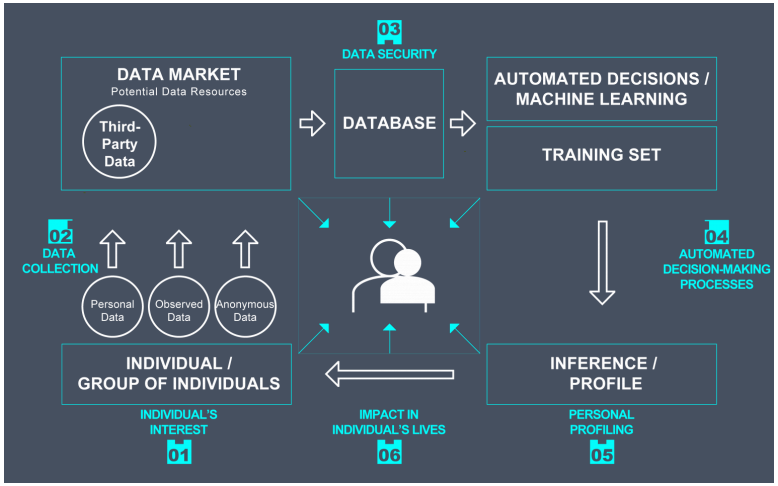
Figure 1: Application of the proposed framework to three apps and the EDPB guidelines, as indicated in each panel. The numbers represent each of the criteria, and the compliance with the criteria from the three main groups are shown in the outer circle.

"A socio-technical framework for digital contact tracing" R. Vinuesa, A. Theodorou, M. Battaglini, V. Dignum arXiv preprint arXiv:2005.08370, 2020
https://arxiv.org/pdf/2005.08370.pdf

10. App easy to deactivate/remove. Either through clear instructions or automatically by sunset clause
11. Open-Source code. Participatory and multidisciplinary development, access to the code.

C. GOVERNANCE.

12. Public Ownership. Avoid private initiative.
13. Data governance should be made public.
14. Downloading the app needs to be voluntary.
15. Sunset Clause.
16. Legislation and Policy. Clear, broader legal framework
17. Incidental Findings and dual-use policy. Purposes beyond contact tracing.
18. Design Impact Assessment and Open Development Process.
19. Right to contest and demand human intervention.



01. User needs

02. Data Collection

03. Security

04. ADM/Algorithm

05. Inferences/Profiles

06. Impact in user's lives

A) ETHICS OF DATA COLLECTION AND COMMUNICATION

1. **Technological resources – Surveillance.**
2. Transparency and Awareness about
   - i. **Observed data**
   - ii. **Third-Party data**
   - iii. **Misuse of information and data repurpose**
3. Failure in **Data Minimization Principle**: Collecting more personal data than necessary to achieve the purpose.
4. Unilaterally alter **Terms of Service** (ToS) agreements and **Privacy Policies.**
5. **Lack of control** over own personal data. Not possibility of opting-out.

B) ETHICS OF DATA PROCESSING

Issues for (i) collection and (ii) analysis of large datasets.

1. **Re-identification of individuals**
   Identification of types of individuals, from **group discrimination** (e.g. ageism, racism, sexism).
2. **Low and poor data quality**, that results in inaccurate results.
3. Storing personal data for **repurposing** reasons. Failure in compliance principle storage limitation.
4. Pseudonymization, anonymization and encryption.

C) ETHICS OF ALGORITHMS

1. **Opacity**, when not known how patterns are obtained and future behaviors of individuals, or groups of individuals, are predicted.
2. **Discriminations and biases** when data training sets for algorithm are e.g. irrelevant, inaccurate, incomplete or insufficiently accurate, and when they respond to the discriminatory biases of organizations.
3. **No access to profiles**
4. **Auditability of algorithms.**

D) ETHICS OF PRACTICES

1. **Unsolved** informed and explicit **consent.**
2. **Misuse** of personal data, or used for **incompatible purposes**.
3. **Identity theft (Face Recognition Technology)**
4. **Privacy invasion** due to technology use.
5. **Impact on individuals**, or group of individuals, discriminatory or biased inferences and profiling
6. **Transparency:** WHAT information should be made transparent and to WHOM should it be disclosed.

Thank you