Privacy and Digital Rights in the Time of COVID-19; apps & beyond

UK IGF
September 2020

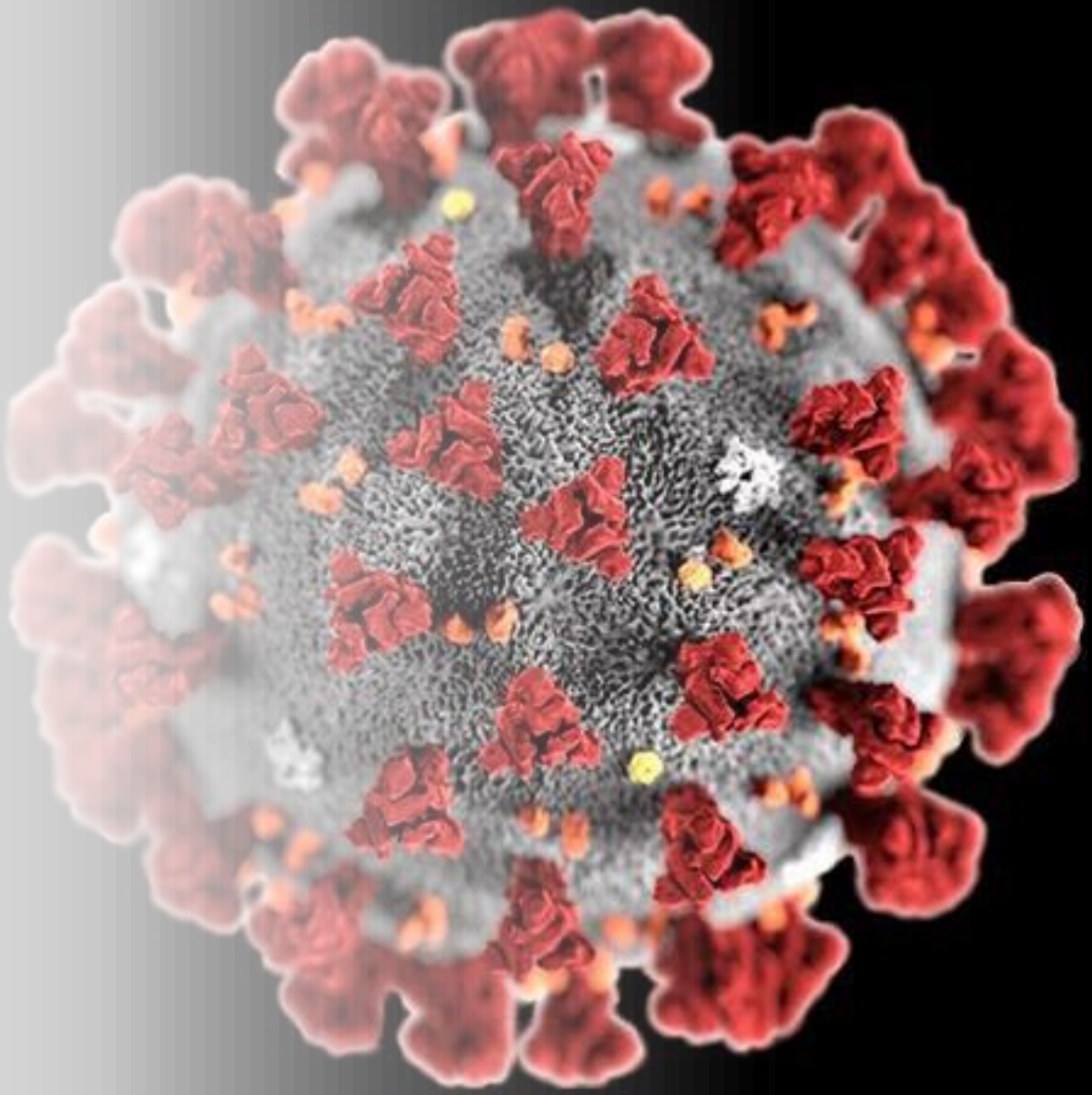
Lilian Edwards

Professor of Law, Innovation and Society

Newcastle Law School

Lilian.edwards@ncl.ac.uk

@lilianedwards



Three COVID-19 surveillance technologies

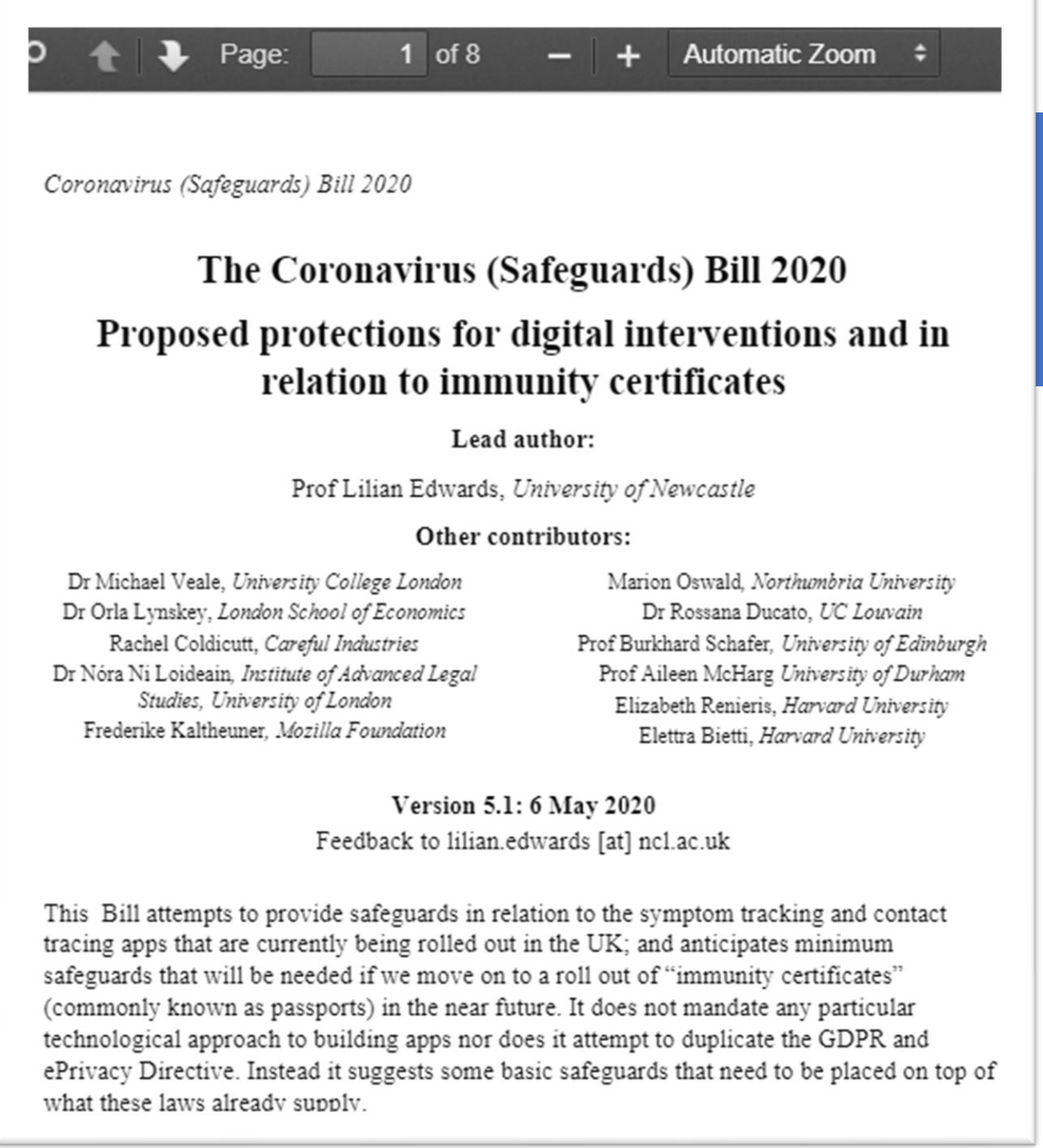
- 1. State sponsored “contact tracing” apps (proximity detection & warning apps)
- 2. Extended private sector surveillance
  - Workplace
  - Campus
- 3. Digital IDs (health status)
- Impact on user rights? (privacy, speech, assembly)

1/ Contact Tracing Apps ("Proximity Tracing) & the Privacy Monster

- NHSX "centralised" app conceived March 2020 as central tent-peg "world-beating" of E&W tracing strategy
- Google/Apple protocol announced April 10 2020
- Test and Trace including manual tracing as overarching umbrella replaced concentration on app
- English App v1 ceased development 18 June 2020
- NI Gapple app, 31 July 2020
- Scottish Gapple app, 10 September 2020
- What next?

- Effect on digital and user rights?

- **Legal** regulation in relation to **data protection** remained with Information Commissioner's Office (ICO)
- **Other aspects?**
- **"Ethical" Governance** – freestanding NHSX app Ethics Advisory Board, stood down in June - > JBC?



Contact tracing apps

- Sufficient legal protections from data protection (GDPR/DPA 2018)?
  - *Retention* of data till when? (storage limitation)
  - *Sharing with who?*
  - *Automated decision making?*
- Pivot to decentralised G/Apple app
  - Considerably less danger of personal data being collected, retained, shared by state
- What are the key remaining issues **now**?

Remaining worries with state proximity apps

Model Coronavirus Safeguards Bill 2020

1. Voluntary : No one shall be penalised for not having a phone (or other device), leaving house without a phone, failing to charge phone, turning off Bluetooth, etc

2. No coercion/discrimination: No one shall be compelled to install a symptom and contact tracing app, or to share messages of their status on such an app on request (eg to an employer, insurer, shop, transport or service provider)

Existing UK Equality Act 2010?

Rests on "protected characteristics" – which do not include health, or Coronavirus status (tho do include "disability") (*indirect* discrimination based on a protected characteristic like race?)

Later apps such as Scottish are publishing DPIAs, Equality Impact Assessments, Human Rights Impact Assessments, Fairer Scotland Duty

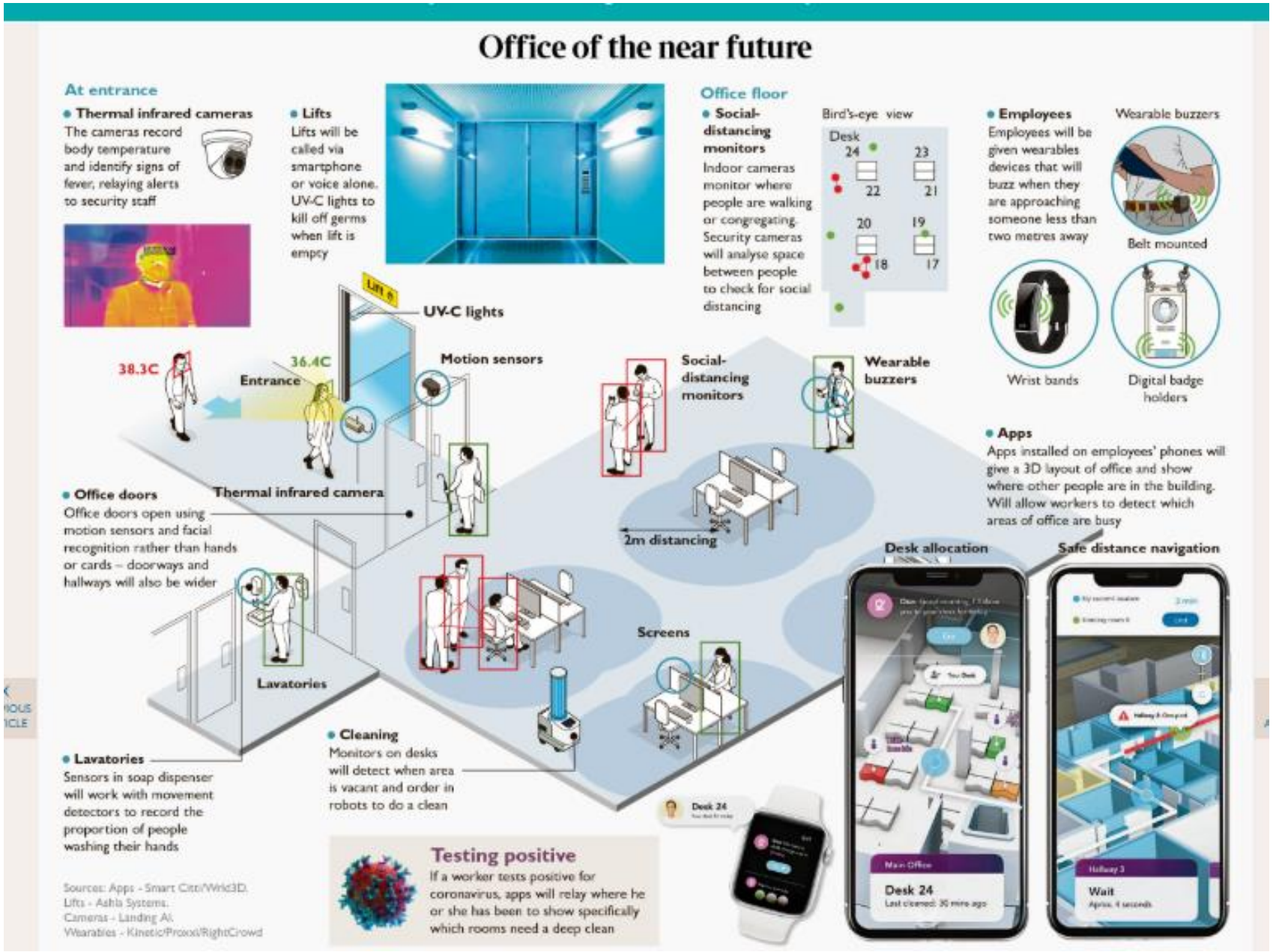
Part 2 Equality: key concepts

Chapter 1 Protected characteristics

4. The protected characteristics
5. Age
6. Disability
7. Gender reassignment
8. Marriage and civil partnership
9. Race
10. Religion or belief
11. Sex

2. Privatised Surveillance

a. Workplace



The Times,June 08 2020

https://www.thetimes.co.uk/edition/news/coronavirus-app-will-tell-workers-if-its-safe-to-go-to-the-lavatory-qkgq3ppbg

Issues?

- **Fits into existing exacerbating trends of surveillance**
  - *Integration into/extending existing workplace surveillance*
    - CCTV, interception web/ telephone, Google-searching, asking for social media credentials, wearables as “wellness” and performance management
  - *Integration into existing algorithmic profiling for workplace*
    - automated hiring, firing, promotion, discipline – already dubious from DP point of view (https://arxiv.org/abs/1910.06144)
- **Much worse for privacy/autonomy than G/Apple contact tracing apps!**
    - largely identifying, not privacy-preserving;
    - mandatory via contract;
    - little control over employers policies
    - **blurring work/life balance (work from home conferencing)**
    - **little legal restraint by DP law on lawful basis**, even re sensitive health or biometric data (see also interception of workplace communications)

b. Campus COVID-19 Surveillance

TECHNOLOGY

The Pandemic Is No Excuse to Surveil Students

Trying to do so is all but useless.

ZEYNEP TUFEKCI SEPTEMBER 4, 2020

Privacy invasive

- Using campus network or Eduroam logins for location surveillance of individuals
- Wi fi beacon posts in university libraries to check who sat near who
- Wearables – individual “tracking beacons”

Privacy preserving

- Wastewater/ sewage analysis
- Pooled testing
- CO2 measurements for aggregate occupancy of spaces (PLASMA at Newcastle)
- Blurred CCTV
- “Heatmaps” of areas of high risk to avoid

3. From immunity passports to “public health identities”

- Severe worries about discriminatory potential, “societal stratification”, privacy, perverse incentives
  - Kofler & Baylis “Ten reasons why immunity passports are a bad idea”, Nature, 2020
- Concerns about accuracy/utility, but revival of interest in UK right now?
- General post-Cummings moves towards greater data sharing across gov -> profiling of status?
- Digital Identity Strategy Board“**Next steps outlined for UK’s use of digital identity”,** Sept 1 2020
- Hancock: “health status” as future for app ; when were you last tested? on app in mass testing scenario

“An emerging aspect is the development of a ‘Public Health Identity’ (PHI), a system for verifiably sharing private health data relevant to public health concerns. These can come in the form of a health status app or digital immunity certificate, which could be used to stream society based on an individual’s health or risk of COVID-19 infection or transmission. Streaming could formally or informally shape how citizens access parts of society, with possible employment, spaces, travel or interaction contingent on bringing personalised private health data into the public sphere. “

“The issues arising from ‘streaming society’ – whether through social nudges or legal requirements – around a health status … may generate or exacerbate existing inequalities, or lead to stigma or discrimination which may be hard to undo. ”

https://www.adalovelaceinstitute.org/our-work/identities-liberties/a-public-health-identity-health-status-apps-immunity-certificates-and-biometrics/