# **COVID-19:** Privacy Deep Dive

**Collin Kurre**
BT plc

**IEEE UK & Ireland** Annual General Meeting
24 April 2020

# **COVID-19** Privacy deep dive

BBC NEWS

Technology

## Coronavirus: Privacy in a pandemic

Rory Cellan-Jones
Technology correspondent
@BBCRoryCJ

2 April 2020

Coronavirus pandemic

FINANCIAL TIMES

Latest on Coronavirus

Coronavirus latest: German biotech firm granted vaccine go ahead

Netflix: takeover TV Premium

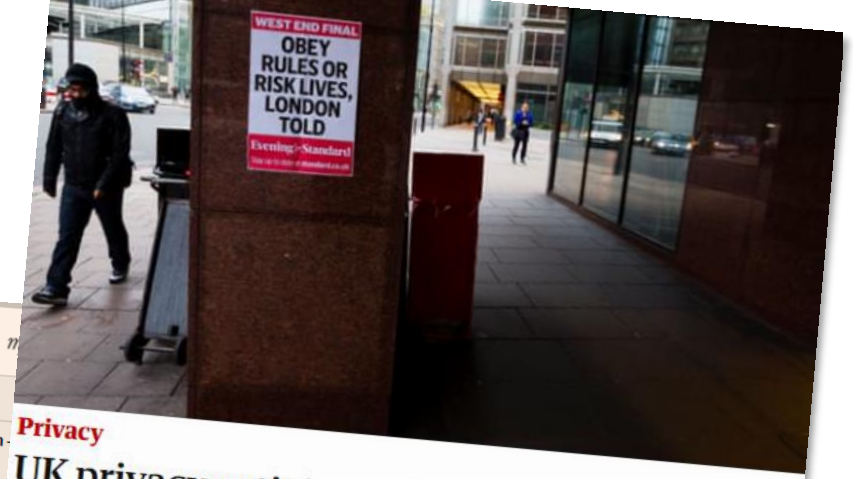
Food scarcity is not the problem - poverty is Premium

Coronavirus Business Update Coronavirus

+ Add to myFT

## Contact-tracing apps raise surveillance fears

Mobile phone data could be vital tool for reopening economies




Privacy

## UK privacy activists raise fears over social distancing tracking

**Mobile phone operators' data could be used to monitor success of coronavirus policy**

THE WALL STREET JOURNAL.

SUBSCRIBE SIGN IN

TECH

## To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits

Geolocation and facial-recognition systems can locate vectors of infections, but they also gather highly personal data

The New York Times

The Coronavirus Outbreak

LIVE Latest Updates Should I Wear a Mask? Maps Markets W

## *For Autocrats, and Others, Coronavirus Is a Chance to Grab Even More Power*

Leaders around the world have passed emergency decrees and legislation expanding their reach during the pandemic. Will they ever relinquish them?

EURACTIV

LATEST: CORONAVIRUS | What is happening in Europe - Stay updated with the tracker from our media network

Sections

Home / News / Digital / Data protection / Privacy activists on COVID-19 surveillance: Either ineffective or questionable

## Privacy activists on COVID-19 surveillance: Either ineffective or questionable

By Philipp Grüll | EURACTIV.de | translated by Sarah Lawton

26 Mar 2020 (updated: 31 Mar 2020)





BT

# **COVID-19** Privacy deep dive

I. **Human rights impacts of COVID-19**
II. Privacy vs. Data Protection
III. How is data being used in pandemic response?
IV. Response: “Disaster privacy, or privacy disaster”?
V. Discussion

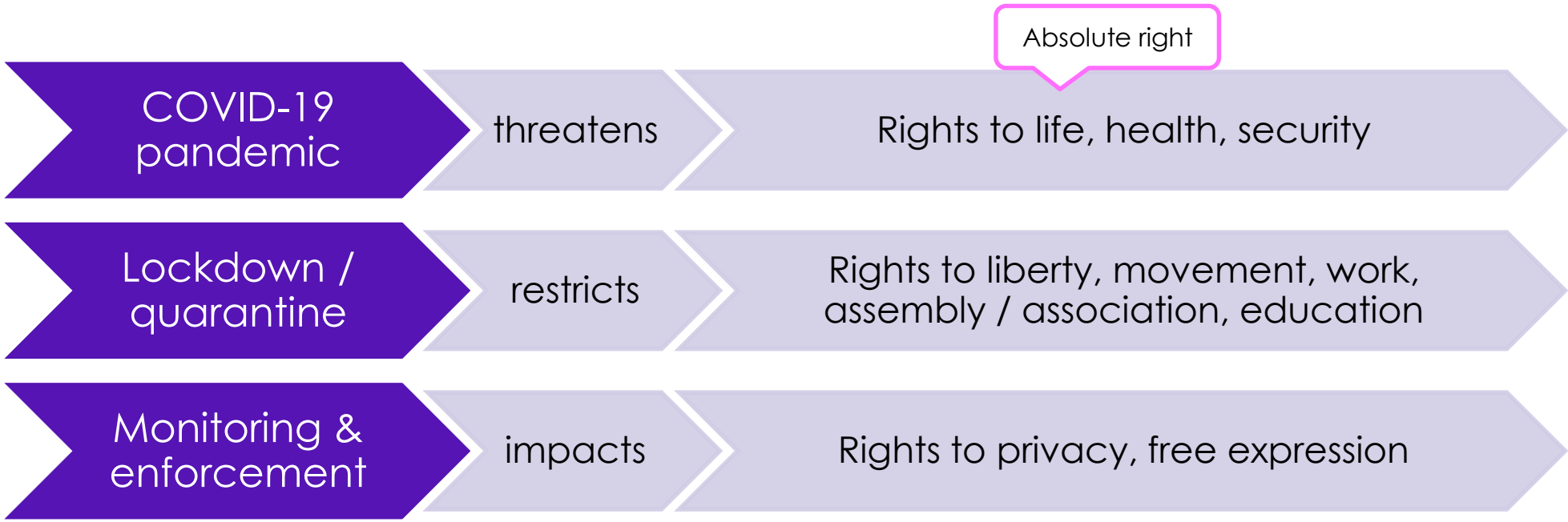

Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

# **COVID-19** Human rights impacts

"Invoking human rights does not determine the dilemma. Human rights principles, however, provide the vocabulary for the evaluation of the decision-making process."

*Andrew Clapham*
*Former Amnesty International Rep to the UN*

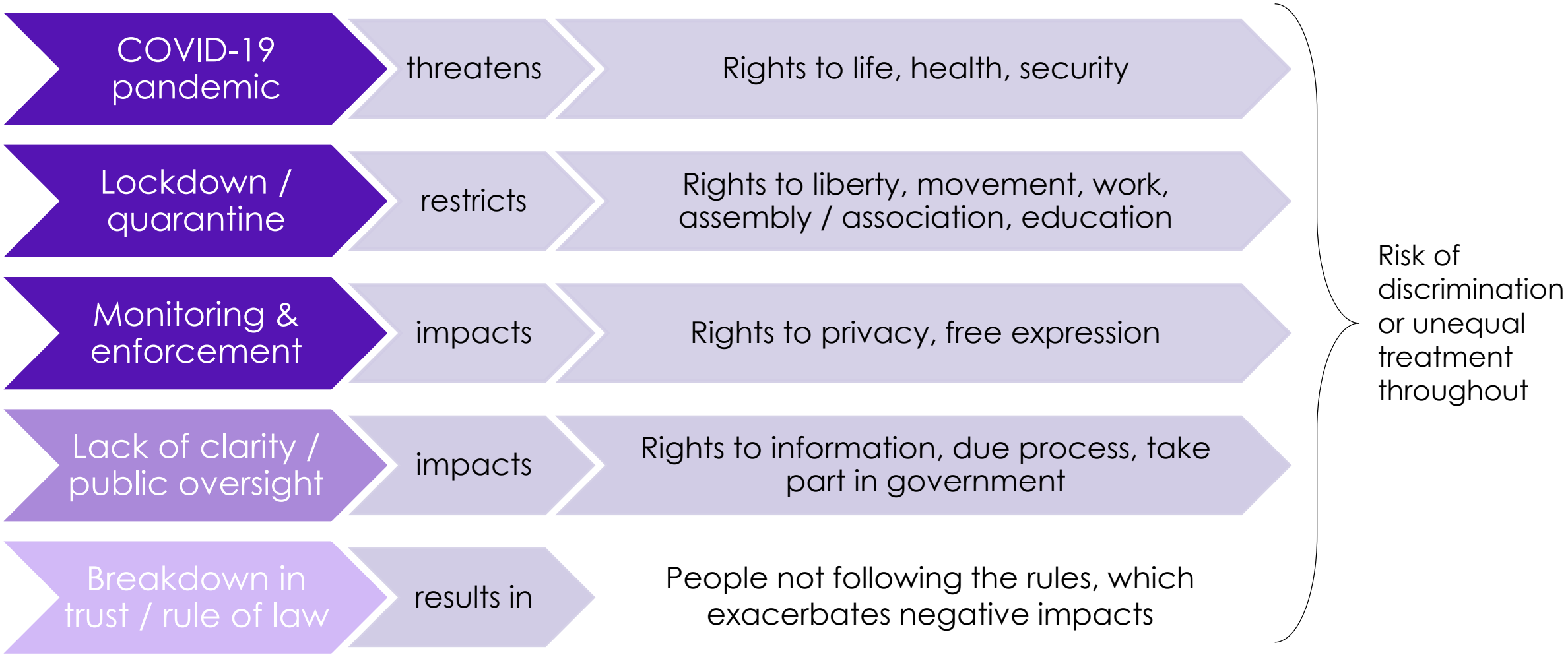
# **COVID-19** Human rights impacts






Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

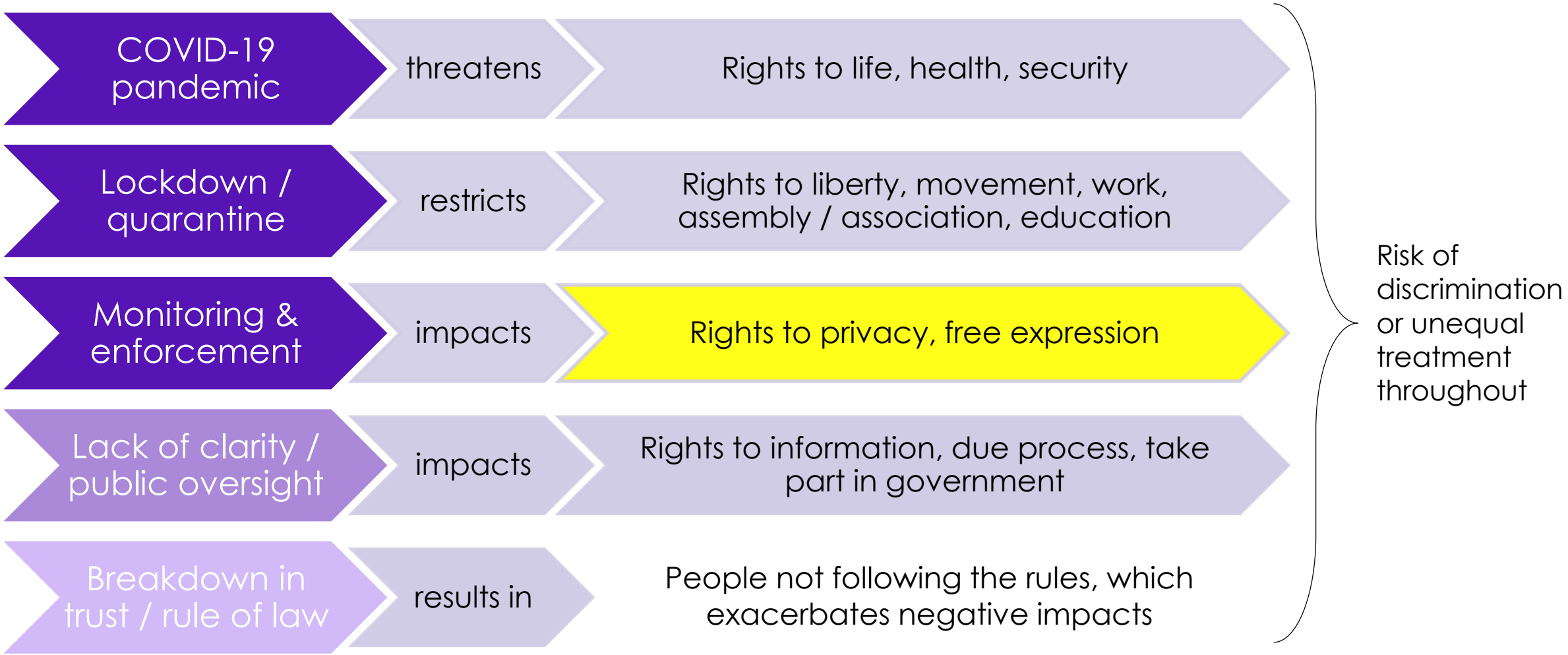
# **COVID-19** Human rights impacts






Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

# **COVID-19** Human rights impacts






Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

# **COVID-19** Privacy deep dive

I. Human rights impacts of COVID-19

**II. Privacy vs. Data Protection**

III. How is data being used in pandemic response?

IV. Response: "Disaster privacy, or privacy disaster"?

V. Discussion

# What is the **right to privacy**?

Key elements:

1. Desire to be free from observation
2. Desire to restrict circulation of information about ourselves
3. Interest in being able to communicate with others without third parties eavesdropping
4. Need to protect our physical and mental well-being
5. Belief that space should be made to develop our personalities free from control

# And what about **data protection**?

Main principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

# And what about **data protection**?

### Your right to be informed if your personal data is being used

An organisation must inform you if it is using your personal data.

### Your right to get copies of your data

You have the right to find out if an organisation is using or storing your personal data.


### Your right to get your data corrected

You can challenge the accuracy of personal data held about you by an organisation.

### Your right to get your data deleted

You can ask an organisation to delete personal data that it holds about you.

### Your right to limit how organisations use your data

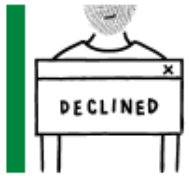
You can limit the way an organisation uses your personal data.

### Your right to data portability

You have the right to get your personal data from an organisation in a way that is accessible .

### The right to object to the use of your data

You have the right to object to the processing or use of your personal data in some circumstances.




### Your rights relating to decisions being made about you without human involvement

Decisions are made about you when your personal data is processed automatically.

### Your right to access information from a public body

Make a request for information from a public body.

### Your right to raise a concern

Tell an organisation if you're concerned about how they are using your data.

Image source:
UK Information Commissioner's Office
https://ico.org.uk/your-data-matters/





BT

# **Privacy** and **Data Protection**

## Privacy

Key strength: adaptability

Needs and expectations based on context, constantly reassessed

Key challenge: social value

Weight of privacy against other trade-offs varies between individuals and societies

## Data Protection

Key strength: enforceability

Processes and obligations for compliance more clearly defined

Key challenge: scope

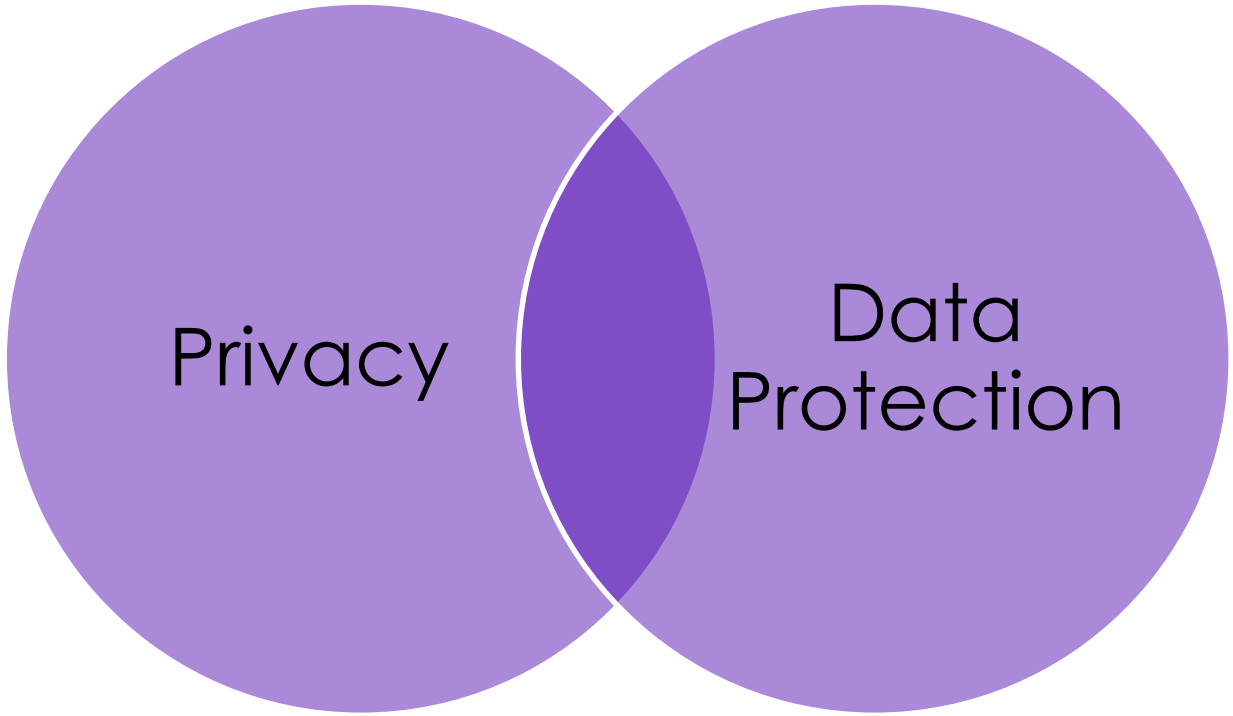
(re)Defining "personal info" in light of new tech / data collection (e.g. inferences)



Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

BT

# **Privacy** and **Data Protection**




- Governance
- Transparency
- Engagement
- Safeguards
- Oversight mechanisms
- Channels for complaint / redress

…**fair information practice**



Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

BT

# **COVID-19** Privacy deep dive

I. Human rights impacts of COVID-19

II. Privacy vs. Data Protection

**III. How is data being used in pandemic response?**

IV. Response: "Disaster privacy, or privacy disaster"?

V. Discussion

# **COVID-19** Data sharing

Date **28 March 2020**

Type **Statement**

The ICO's Deputy Commissioner Steve Wood said:

> "Generalised location data trend analysis is helping to tackle the coronavirus crisis. Where this data is properly anonymised and aggregated, it does not fall under data protection law because no individual is identified.
>
> "In these circumstances, privacy laws are not breached as long as the appropriate safeguards are in place.

# Can data be **anonymous**?

Some anonymization techniques do not provide sufficient privacy protection for personal data because they can be reverse engineered relatively easily:

- **Suppression / scrubbing**: Removing data deemed to be personally identifiable from data set (e.g. name or address fields)

- **Pseudonymization**: Replacing one unique identifier with another so the individual isn't directly identified

# Can data be **anonymous**?

Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization

*UCLA Law Review, Vol. 57, p. 1701, 2010*
*U of Colorado Law Legal Studies Research Paper No. 9-12*

77 Pages • Posted: 13 Jul 2012 • Last revised: 22 Feb 2015

Paul Ohm
Georgetown University Law Center

Date Written: August 13, 2009

nature communications

Article | Open Access | Published: 23 July 2019

PDF

**Estimating the success of re-identifications in incomplete datasets using generative models**

Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye

*Nature Communications* **10**, Article number: 3069 (2019) | Cite this article

**99k** Accesses | **23** Citations | **2098** Altmetric | Metrics

TC

**Researchers spotlight the lie of 'anonymous' data**

Natasha Lomas @riptari / 11:30 am BST • July 24, 2019

The New York Times

***Your Data Were 'Anonymized'? These Scientists Can Still Identify You***

Computer scientists have developed an algorithm that can pick out almost any American in databases supposedly stripped of personal information.

**Twelve Million Phones, One Dataset, Zero Privacy**

By Stuart A. Thompson and Charlie Warzel

DEC. 19, 2019

534

EVERY MINUTE OF EVERY DAY, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files. The Times Privacy Project





BT

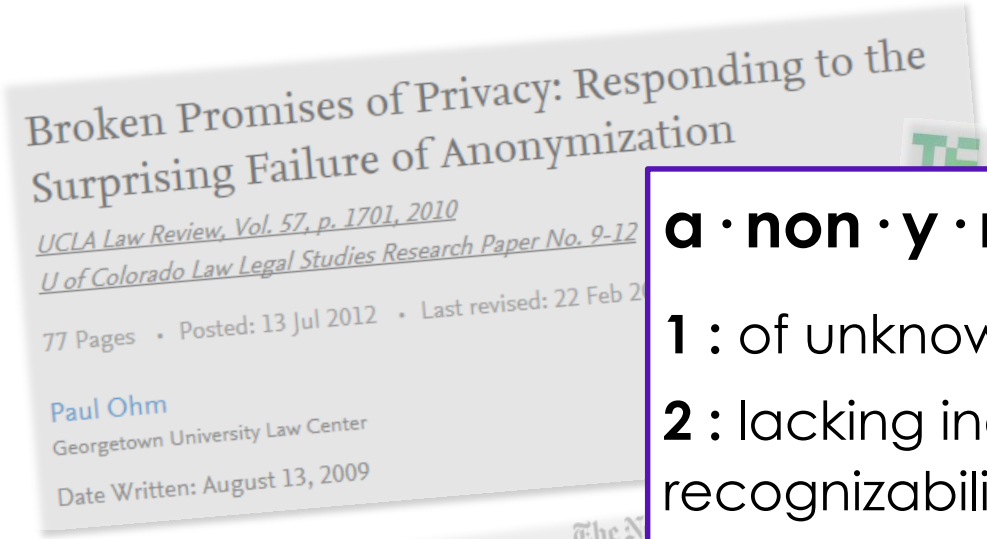
# Can data be **anonymous**?

**a · non · y · mous** | ə-ˈnä-nə-məs

**1 :** of unknown authorship or origin

**2 :** lacking individuality, distinction, or recognizability

**3 :** not named or identified


Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization

UCLA Law Review, Vol. 57, p. 1701, 2010
U of Colorado Law Legal Studies Research Paper No. 9-12

77 Pages • Posted: 13 Jul 2012 • Last revised: 22 Feb 2

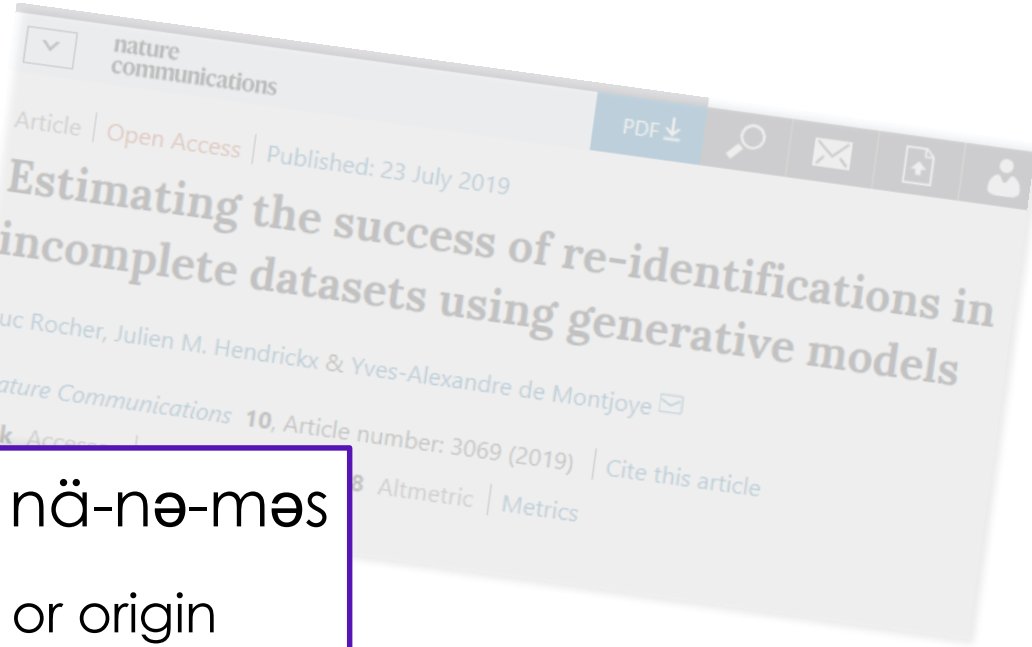
Paul Ohm
Georgetown University Law Center

Date Written: August 13, 2009


Your Data Were
Scientists Can Still Identify You

Computer scientists have developed an algorithm that can pick out almost any American in databases supposedly stripped of personal information.




nature communications

Article | Open Access | Published: 23 July 2019

Estimating the success of re-identifications in incomplete datasets using generative models

Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye

Nature Communications 10, Article number: 3069 (2019) | Cite this article

99k Altmetric | Metrics


welve Million Phones, One Dataset, Zero Privacy

By Stuart A. Thompson and Charlie Warzel

DEC. 19, 2019

534

EVERY MINUTE OF EVERY DAY, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files. The Times Privacy Project





BT

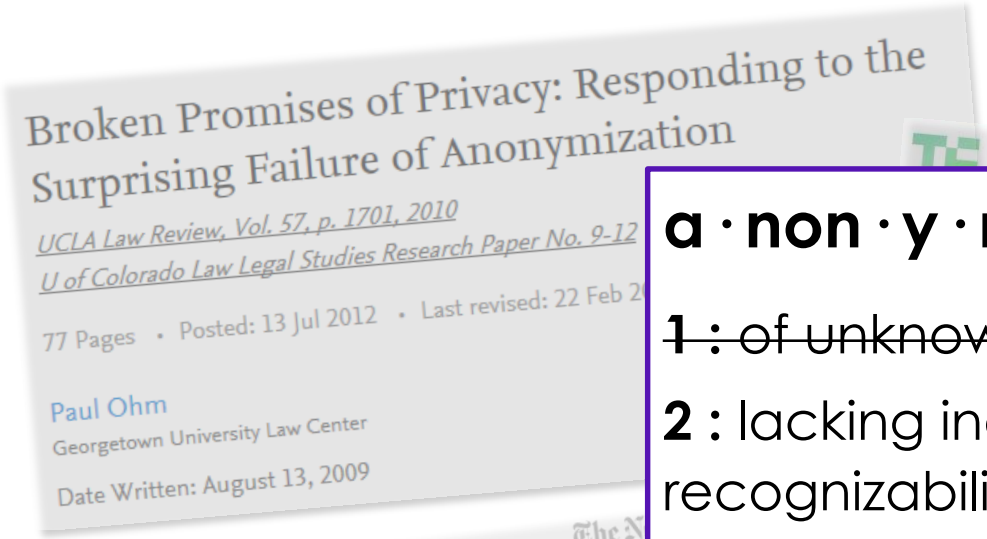
# Can data be **anonymous**?

**a · non · y · mous** | ə-ˈnä-nə-məs

~~**1 :** of unknown authorship or origin~~

**2 :** lacking individuality, distinction, or recognizability

**3 :** not named or identified


Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization

UCLA Law Review, Vol. 57, p. 1701, 2010

U of Colorado Law Legal Studies Research Paper No. 9-12

77 Pages • Posted: 13 Jul 2012 • Last revised: 22 Feb 2

Paul Ohm

Georgetown University Law Center

Date Written: August 13, 2009


Your Data Were
Scientists Can Still Identify You

Computer scientists have developed an algorithm that can pick out almost any American in databases supposedly stripped of personal information.




nature communications

Article | Open Access | Published: 23 July 2019

Estimating the success of re-identifications in incomplete datasets using generative models

Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye

Nature Communications 10, Article number: 3069 (2019) | Cite this article

Altmetric | Metrics


welve Million Phones, One Dataset, Zero Privacy

By Stuart A. Thompson and Charlie Warzel

DEC. 19, 2019

534

EVERY MINUTE OF EVERY DAY, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files. The Times Privacy Project





BT

# Can data be **anonymous**?

**a · non · y · mous** | ə-ˈnä-nə-məs

~~**1 :** of unknown authorship or origin~~

~~**2 :** lacking individuality, distinction, or recognizability~~

**3 :** not named or identified

Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization

*UCLA Law Review, Vol. 57, p. 1701, 2010*
*U of Colorado Law Legal Studies Research Paper No. 9-12*

77 Pages • Posted: 13 Jul 2012 • Last revised: 22 Feb 2

Paul Ohm
Georgetown University Law Center

Date Written: August 13, 2009

nature communications

Article | Open Access | Published: 23 July 2019

Estimating the success of re-identifications in incomplete datasets using generative models

Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye

*Nature Communications* **10**, Article number: 3069 (2019) | Cite this article

Altmetric | Metrics

Your Data Were ... Scientists Can Still Identify You

Computer scientists have developed an algorithm that can pick out almost any American in databases supposedly stripped of personal information.

Twelve Million Phones, One Dataset, Zero Privacy

By Stuart A. Thompson and Charlie Warzel

DEC. 19, 2019

534

EVERY MINUTE OF EVERY DAY, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files. The Times Privacy Project

# Can data be **anonymous**?


**“functional non-identifiability”**





BT

# Anonymity through **Randomization**

Alters data to remove strong links between data and individuals.

Techniques:

- **Noise addition** – adding bogus data to make the data less accurate to a specified degree (e.g. +/- 3%)
- **Permutation** – shuffling values so they're artificially linked to different data subjects
- **Differential privacy** – generating anonymized views of particular datasets while retaining an original copy

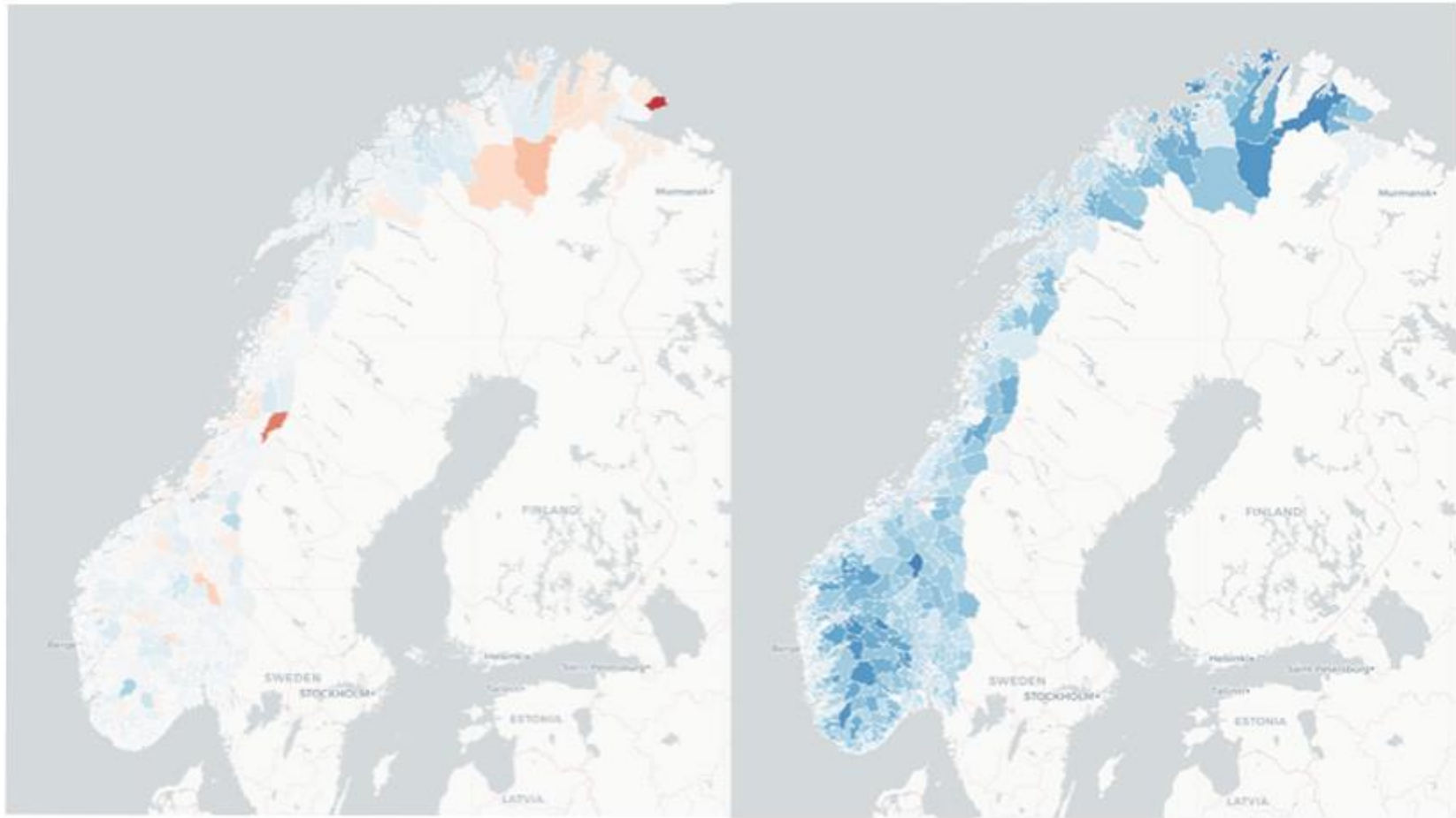
# Anonymity through **Generalization**

Dilutes attributes of data subjects by including them into groups and giving summary statistics, not raw data.

Techniques:

- **Aggregation / K-anonymity** – groups data subject with at least ‘k’ other individuals (20, 50, etc), meaning the probability of two records corresponding is 1/K
- **L-diversity** – builds on this aggregation by making sure that each group has at least ‘l’ different values
- **T-closeness** – takes it even further, seeking to create equivalent groups that mimic the initial distribution of the original dataset

# **COVID-19** Data sharing




The maps show people's movement in Norway on 10 March (left) and 15 March, compared to people's movement on the same day the previous week. The blue color a decrease in movement. "I have never before witnessed such a massive drop in people's movement, as we are seeing now," says Engø-Monsen.

# **COVID-19** Privacy deep dive

I. Human rights impacts of COVID-19

II. Privacy vs. Data Protection

III. How is data being used in pandemic response?

**IV. Response: "Disaster privacy, or privacy disaster"?**

V. Discussion



Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

BT

# **COVID-19** Privacy deep dive

## Disaster Privacy/Privacy Disaster

20 Pages • Posted: 29 Jul 2019

### Abstract

Privacy expectations during disasters differ significantly from non-emergency situations. Recent scandals, such as inappropriate disclosures from FEMA to contractors, illustrate that tradeoffs between emergencies and privacy must be made carefully. Increased use of social technologies to facilitate communication and support first responders provide more opportunities for privacy infringements, despite increased regulation of disaster information flows to government agencies and with trusted partners of the government. This paper specifically explores the actual practices followed by popular disaster apps. Our empirical study compares content analysis of privacy policies and government agency policies, structured by the contextual integrity





BT

# **COVID-19** Privacy / human rights response

**Big Brother Watch** @BigBrotherWatch

This crisis requires the public's courage and co-operation, not our criminalisation.

These are the most draconian powers ever proposed in peace-time Britain and they require urgent review and reform. /8

#CoronavirusBill #Coronavirus

**Liberty** @libertyhq · Mar 25

280-character **#CoronavirusBillUK** briefing.

Bill must be amended to better protect rights&freedoms, incl:

- 3 month sunset clause
- Judge must authorise detention
- Suspend NHS charges for overseas patients & stop passing data to Home Office
- No relaxation of surveillance rules

**Ada Lovelace Institute** @AdaLovelaceInst · Mar 26

'When one has a hammer—in this case, cellphone tracking—it is tempting to see nails everywhere.'

Using phone data to trace #COVID19 might assist public health responses. But is it effective?

If not, it endagers not only our liberty, but our health too.

Location Surveillance to Counter COVID-19: Efficacy l...
Determining whether surveillance will help combat the virus requires understanding how the coronavirus sp...
lawfareblog.com

# **COVID19** Privacy / human rights response


AMNESTY INTERNATIONAL

EN

DOCUMENT

CENSORSHIP AND FREEDOM OF EXPRESSION

JOINT STATEMENT: STATES USE OF DIGITAL SURVEILLANCE TECHNOLOGIES TO FIGHT PANDEMIC MUST RESPECT HUMAN RIGHTS

2 April 2020, Index number: POL 30/2081/2020

- Data sharing must be lawful, necessary, proportionate, and time-bound
- Governments should publicly disclose data sharing agreements
- Data anonymization processes should be evidenced
- Surveillance in response to COVID19 should not fall under domain of security and intelligence agencies
- Tech should play a role in saving lives at this time, but use of surveillance could undermine trust in government and efforts to fight COVID19





BT

# **COVID19** Industry response

"The mobile industry recognises **the urgency with which governments must act** to slow the spread of COVID-19 and the desire of some governments to seek help regarding those efforts. At the same time, the industry recognises that the **use of mobile network operator data by governments or agencies raises serious privacy concerns**."

GSMA COVID19 Privacy Guidelines

# **COVID19** Privacy / human rights response

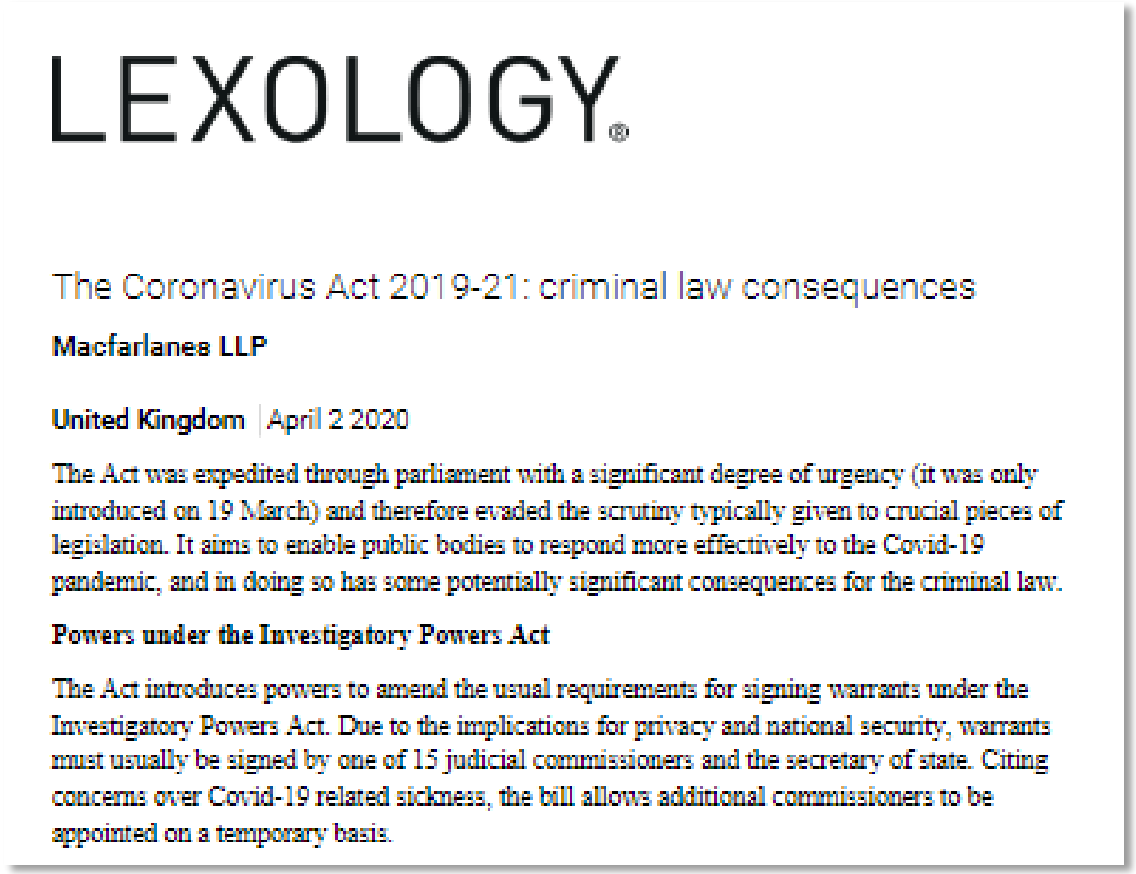





BT

# **COVID19** Legal response

"The debate over these powers likely represents a **harbinger of wider issues to come**, as emergency legislation introduced to deal with an urgent pandemic **clashes with established human rights and data protection legislation.**"



LEXOLOGY®

The Coronavirus Act 2019-21: criminal law consequences

**Macfarlanes LLP**

**United Kingdom** | April 2 2020

The Act was expedited through parliament with a significant degree of urgency (it was only introduced on 19 March) and therefore evaded the scrutiny typically given to crucial pieces of legislation. It aims to enable public bodies to respond more effectively to the Covid-19 pandemic, and in doing so has some potentially significant consequences for the criminal law.

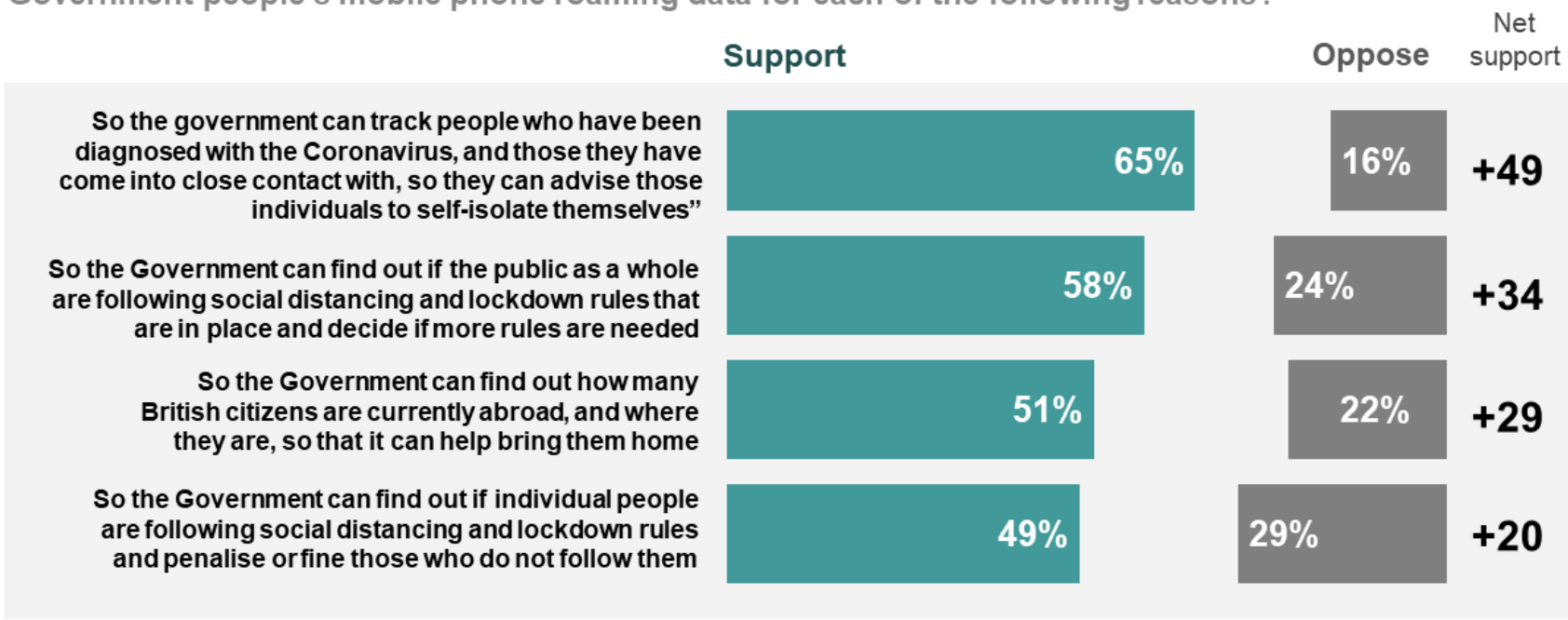
**Powers under the Investigatory Powers Act**

The Act introduces powers to amend the usual requirements for signing warrants under the Investigatory Powers Act. Due to the implications for privacy and national security, warrants must usually be signed by one of 15 judicial commissioners and the secretary of state. Citing concerns over Covid-19 related sickness, the bill allows additional commissioners to be appointed on a temporary basis.

# **COVID19** Public response

## Government surveillance of mobile phone roaming data

How strongly, if at all, would you support or oppose mobile phone service providers giving the Government people's mobile phone roaming data for each of the following reasons?




**Base: 1,069** Online British adults 18-75, 10-13 April 2020

1 © Ipsos | Coronavirus polling | April 2020

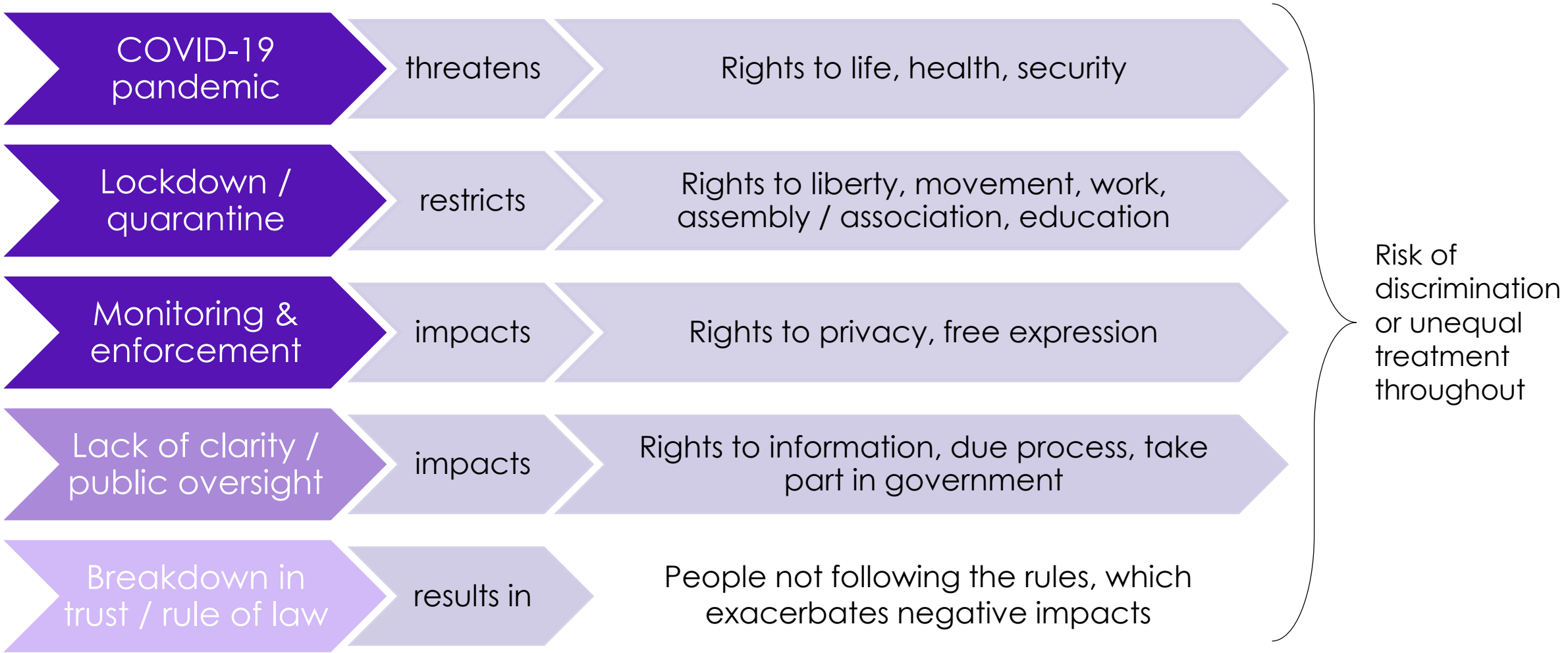
Ipsos MORI





BT

# **COVID-19** Human rights impacts






Collin Kurre. Human / Digital Rights Team. British Telecommunications plc.

# **COVID-19** Privacy deep dive

I. Human rights impacts of COVID-19

II. Privacy vs. Data Protection

III. How data is being used in pandemic response

IV. Response: “Disaster privacy, or privacy disaster”

**V. Discussion** – questions, comments, responses?

# **Works cited** and other resources


**UK Information Commissioner's Office. Statement in response to the use of mobile phone tracking data to help during the coronavirus crisis.** 28 March 2020. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/statement-in-response-to-the-use-of-mobile-phone-tracking-data-to-help-during-the-coronavirus-crisis/

**European Data Protection Supervisor. Opinion 05/2014 on Anonymisation Techniques.** 10 April 2014. https://www.pdpjournals.com/docs/88197.pdf

**Telenor Group. How mobility data can help predict and prevent the spread of COVID-19.** March 2020. https://www.telenor.com/how-our-mobility-data-can-help-predict-and-prevent-the-spread-of-covid-19/

**GSMA. The GSMA COVID-19 Privacy Guidelines.** April 2020. https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy-Guidelines.pdf

**Sanfilippo, Madelyn et al. Disaster Privacy / Privacy Disaster.** 29 July 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427562

**UK Parliament Human Rights Joint Committee. Inquiry into human rights implications of the Government's response to COVID-19.** https://committees.parliament.uk/work/218/the-governments-response-to-covid19-human-rights-implications/

# **Works cited** and other resources


**Amnesty, et al. Joint statement: States use of digital surveillance technologies to fight pandemic must respect human rights.** 2 April 2020. https://www.amnesty.org/en/documents/pol30/2081/2020/en/

**Macfarlanes LLP. The Coronavirus Act 2019-21: Criminal law consequences.** 2 April 2020. https://www.macfarlanes.com/what-we-think/in-depth/2020/the-coronavirus-act-2019-21-criminal-law-consequences/

**Ipsos MORI. Majority of Britons support government using mobile data for surveillance to tackle coronavirus crisis.** 18 April 2020. https://www.ipsos.com/ipsos-mori/en-uk/majority-britons-support-government-using-mobile-data-surveillance-tackle-coronavirus-crisis

**BT Plc. Our customers and supporting the national effort.** April 2020. https://www.btplc.com/coronavirus/Ourcustomers/index.htm


## Further reading


**European Data Protection Supervisor. Data Protection / Privacy Primer.** https://edps.europa.eu/data-protection/data-protection_en

**Andrew Clapham. Human Rights: A Very Short Introduction.** 2015. https://global.oup.com/academic/product/human-rights-a-very-short-introduction-9780198706168

# Additional resources shared by participants:

- Ada Lovelace Institute – “COVID-19 rapid evidence review: Exit through the App Store?” https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/
- Business Insider – “The UK scrambles to launch its COVID-19 contact-tracing app, after getting derailed by Apple and Google” https://www.businessinsider.com/nhsx-contact-tracing-app-derailed-apple-google-bluetooth-system-2020-4?r=US&IR=T
- Lilian Edwards – “The Coronavirus (Safeguards) Bill 2020” https://osf.io/preprints/lawarxiv/yc6xu/
- Newsroom NZ – “NZ considering $100m contact tracing ‘CovidCard’” https://www.newsroom.co.nz/2020/04/17/1132682/nz-considering-100m-contact-tracing-covidcard
- New Statesman Tech – “PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear” https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear
- Serge Vaudenay – “Analysis of DP3T” https://eprint.iacr.org/2020/399.pdf
- Venture Beat – “MIT announces Bluetooth breakthrough in coronavirus-tracing app for Android and iOS” https://venturebeat.com/2020/04/08/mit-announces-bluetooth-breakthrough-in-coronavirus-tracing-app-for-android-and-ios/