EXIT THROUGH THE APP STORE TEA AND TECH 29TH APRIL 2020
Trish Shaw and Mark O'Conor

Thoughts and reflections from the SCL Tea and Tech session to help SCL members navigate this time.

Summarised below is the key Ada Lovelace "Exit through the app store" rapid review policy recommendations which are fundamentally intended for Governments, Policymakers and Tech Providers to build TRUST

TOE(E)S:
Transparency – Government must be transparent about the solutions it implements. Being open about the algorithms deployed, the risk models used, how proximity and duration of a contact are defined, details of where, when and to whom data (personal or not) goes, and how notifications to contacts and the public health bodies work. Whatever tech solution is deployed must be clearly grounded in the overall strategy to fight coronavirus.

Oversight – There should be clear governance and oversight of any tech solutions which are implemented. These are to augment existing manual solutions. Oversight should be formed by both a SAGE (Scientific Advisory Group for Emergencies) and a GATE (Group of Advisors on Tech in Emergencies) forming groups which are diverse, representative, and expert advisors.

Engagement – Effective policy interventions take into account the social dimension and the societal impact of tech. This means engaging with as broad a range of actors and those impacted across society, getting them involved in the design, assessment and monitoring of tech solutions.

(Enforcement) – Ensuring that no one is disadvantaged through the use or not use of the App and the data derived from it. That it is not used to unreasonably and inappropriately punish or disadvantage people, and if people do experience harm (including false positives or false negatives) that there is a means of redress.

Safeguards – Legislation should be put in place to ensure that any tech solutions are: (i) purpose limited, (ii) time limited, (iii) with clear mechanisms to prevent mission creep, (iv) clear about uptake and use being voluntary and not mandatory, (v) no civil or criminal sanctions for having a legacy (i.e. not having a Bluetooth enabled) device or for simply not carrying a device on your person, and (vi) clear on what happens to the data (even non-personal data).

Pre-conditions:
There are certain pre-conditions (assumptions and dependencies) which are required to be met for the efficacy of any Contact Tracing App, these are:

Precursor: For any tech solution to be effective, it must be employing the right tool. We need to be assured that COVID19 is transmitted through contact before considering employing a contact tracing App.

(1) You must have a bluetooth enabled device and you must carry it with you as a proxy for you as a person.
(2) Based on a voluntary roll-out, you must have downloaded the App and adhere to its instructions.
(3) Based on a voluntary roll-out, the contact you are in the proximity of must also have downloaded the same App and adhere to its instructions.
(4) The App must be complemented by a strategy of widespread testing for the virus. It must be a given that there be self-isolation from time of the test until the time of the results of the

test, so no intermittent infection could have occurred. It must be clear how accurate or not the testing is.

(5) Accuracy of the reporting. Bad data in caused bad data out. Will the App be reliant of self-reporting based on a symptom tracker or will it require a health professional to report you as infected with COVID-19. Can that reporting be intercepted, made fraudulently, audited.

(6) Financial support measures need to be in place to ensure social compliance with the interventions proposed through notifications on the App. You will not stay at home, self-isolate or quarantine if you do not have the means to feed yourself or pay energy bills etc if you are not able to go to work.

Ethical and societal considerations

We need to be cognisant of the ethical and societal implications of the tech solutions that is being deployed. There is a risk of:

- Proximity and duration not being correctly tuned with our previous or current social behaviours
- Technological Determinism resulting in under or overreliance on the App
- Digital divide – those that have devices and connectivity can and those that don't can't.
- Two tier society – those that to self-isolate and those that do not need to self-isolate (whether for reasons of age, vulnerability, disability, health disadvantages, poverty, or having immunity or presenting with anti-bodies or not)
- Stigmatisation – social stigmas associated with having had COVID19 or not, downloading the App or not.
- Discovery/Re-indentification of contacts – partly a security or workaround risk, but also the concern of what impact having the information knowledge that the App would bring would have on a person. Whether they are "found out" to be the one who infected a friend/family member/colleague, or they found out they were infected by a friend/family member/colleague, this may bring about anger, guilt, regret, revenge. The impact of this, would be greater if COVID19 impacted you least and the other person worst. If infection were deliberate or that the person had knowledge of their symptoms but did not report them, would that warrant litigation. What if a maleficent deliberately socialised in order to infect others, would that warrant criminal sanctions.
- Social pressure to take up whatever interventions are proposed, and consent not really being voluntarily given.
- Social graphs – your network of contacts being mapped. This in and of itself is a matter of your private sphere of life, but it also poses a risk to individuals or groups of individuals being re-identified, especially when overlaid with geolocation data. Protection against this kind of invasion into the private sphere is what a decentralised app (as opposed to a centralised app) would seek to safeguard.
- Undermining of democracy, fundamental freedoms and creeping in of greater surveillance.
- Normalising of extraordinary emergency measures, such that the sacrifice of individual rights and freedoms becomes socially acceptable if not also socially preferable
- Behaviour modification – we have all adopted and adapted our behaviours to cater for social distancing. Could this be a more permanent behaviour change or habit for us.
- What is the social distancing doing for us and to us? How will this impact our new normal as we exit COVID19?
- Implications of mental health go beyond this time of social distancing. Both for those infected, those who have lost loved ones and friends, and those who have not been infected, there is a risk of PTSD/trauma, anxiety, obsessive compulsive disorder, permanent reduction of social contact, agoraphobia, claustrophobia, and increased rates of suicide or

attempted suicide. This does not even touch upon the other issues associated with safeguarding the vulnerable: neglect and mistreatment of elderly, domestic violence, and child abuse

A framework for an exit strategy

Here are some key questions we as a community should be asking in respect of the tech interventions for an exit strategy:

1. What is the intended purpose? Is it clear and have the risks of dual use and the tech intervention being re-purposed for an unintended purpose been mitigated and/or addressed.
2. How effective will the intervention measure be in achieving that intended purpose?
3. What are the dependencies/contingencies for the intervention to operate and be effective?
4. How can we protect against mission creep?
5. What safety-net is in place to prevent against the rachet effect of the general public getting used to this kind of intervention. Crises are known times for individuals to voluntarily relinquish rights and for democracy to be impacted, and for emergency intervention measures not be reversed
6. Is there a clear plan for the end of the health emergency? What are the criteria that will determine when this crisis is officially over? Is it just defined in terms of lapsed time (6/12/24 months) from the point at which a state of emergency or the tech intervention measures were applied, or defined against measurable metrics?
7. Is there a sunset clause? Should we have a period of 'grace' beyond the end of the health emergency before the tech intervention measures are lifted and protocols cease? If so, has this been clearly communicated to the public? Is it a fixed period, or is it subject to further extension? If so, who can authorise/ratify such extension?
8. How will the tech interventions be desisted? Will it require individual user action to remove the App from their devices? Will it be deleted/sunset automatically? Will it be deleted/deactivated centrally? How will users be notified? (e.g. After reading this message, the App will self-destruct!)
9. What should happen to the data (personal data or non-personal data) that has been collected, collated, aggregated and from which insight has been drawn? Options: (a) Delete all. (b) Keep for research use only to plan for the next health emergency/pandemic, or (c) another purpose? Is the purpose for retention clear? Is it clear who will hold it, where and who else will have access to it?
10. When, how and who will audit that the use of the data and the tech intervention measures applied were done so in a reasonable, proportionate, adequate, data minimising manner during the health emergency/pandemic? When, how and who will govern ongoing use of the data and/or the tech intervention measures
11. Planning for the next pandemic or a relapse of this one, when, if and what tech and other intervention measures should be reactivated? What will be the criteria? How will this be communicated to the public.

If the UK is to adopt any technological tool like contact tracing, one thing is clear. ”***There can only be one*** [App]”. If there are multiple apps it will not least be confusing for citizens but will fragment the digital response, leaving the UK divided and conquered - Public trust undermined. The EU is trying to avoid this by having a joined-up approach.

Despite Single Market changes afoot, the UK would be wise to collaborate with EU. If we are in for the long haul with COVID19, then we need to be prepared (for at least our Apps) to be able to talk to our European counterparts!

USEFUL ADDITIONAL READING:

Australia's announcement of deployment of CovidSafe based on Singapore's Trace Together (centralized) app: https://www.bbc.co.uk/news/world-australia-52433340
https://www.theverge.com/2020/4/26/21237598/australia-coronavirus-contact-tracing-privacy

NHSx announcement about contact tracing (centralized) app 24 April 2020 - https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/

ICO statement in response to NHSx announcement on 24 April 2020: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/statement-nhsx-contact-tracing-app/

The Coronavirus (Safeguards) Bill 2020 Proposed protections for digital interventions and in relation to immunity certificates Lead author: Prof Lilian Edwards, University of Newcastle - https://osf.io/preprints/lawarxiv/yc6xu/ version 3 last updated 21 April 2020

European Data Protection Board Guidelines 04/2020 onthe use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

ICO's Opinion on the Apple and Google joint initiative on COVID-19 contact tracing technology 17 April 2020 - Reference: 2020/01 - https://ico.org.uk/media/2617653/apple-google-api-opinion-final-april-2020.pdf

ICO Elizabeth Denham blog on COVID19 apps with decentralized method preferable 17 April 2020
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/

COE - AI Breakfasts: Covid-19 - Myths and realities of tracking applications Council Of Europe on 16 April 2020: https://www.youtube.com/watch?v=l9d3B6AuvdI&feature=youtu.be

eHealth Network - Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States version 1.0, 15 April 2020 -
https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Joint European Roadmap towards lifting COVID-19 containment measures published by the EU commission and European Council on 15 April 2020
https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

Future of Privacy Forum's list of resources: https://sites.google.com/fpf.org/covid-19-privacy-resources/#h.p_l4tfppxBBjkU

The Future for Privacy Forum comparative study table:
https://fpf.org/wp-content/uploads/2020/04/DP3T_The-Role-of-Mobile-Apps-Chart-10.pdf

Trish Shaw is an SCL Trustee and is CEO and Founder of Beyond Reach, a Tech Ethics Consultancy and **Mark O'Conor** is the SCL Chair and Partner & Chair of the London Client Group at DLA Piper (UK) LLP.