Europe Technology Policy Committee

Association for Computing Machinery
acmpo@acm.org | @acmpolicy
www.acm.org/public-policy/europe-tpc

5 May 2020

STATEMENT ON ESSENTIAL PRINCIPLES AND PRACTICES FOR COVID-19 CONTACT TRACING APPLICATIONS

The rapid emergence and spread of the SARS-CoV-2 virus and COVID-19 infection has caused governments around the globe to order a large part of the world's population into various levels of lockdown. These governments now contemplate when and by what means to ease or lift such restrictions without causing a rebound effect wherein the epidemic again starts to spread. In the absence of a cure or vaccine, epidemiologists recommend a combination of measures, including social distancing, large-scale testing, and contact tracing to identify those who have been in contact with infected persons.

Various contact tracing applications have been presented as a means to automate and scale to entire populations surveillance normally done through time-consuming human investigation. These applications rely on the use of Bluetooth wireless technology to identify when two smartphones have been in close proximity for a designated length of time.[1]

The Europe Technology Policy Committee of the Association for Computing Machinery (Europe TPC) is committed to providing technical information to policymakers and the general public in the service of sound public policy formation. With respect to contact tracing systems under active consideration, Europe TPC finds that:

- While all presently proposed contact tracing protocols can be technologically refined to maximize privacy and anonymity,[2] such apps remain highly vulnerable to attack.[3] Accordingly, ***at this time known contact tracing apps cannot fully preserve individual privacy and anonymity;***

[1] Phones equipped with such software exchange identifiers so that they can maintain a record of the phones with which they have been "in contact." When an individual is identified as having been infected, the phones with which the infected person's phone have been in contact are notified so that their owners can take appropriate measures. The DP-3T protocol takes a "decentralized" approach (the identifier of the "infected phone" is uploaded to a central server and broadcast to all other phones, which can then look for a match in their list of recent contacts). The ROBERT protocol employs a "centralized" method (phones whose owners are declared to be infected upload their lists of recent contacts to a central server so that those phones can be notified).

[2] For example, unique numerical identifiers can be randomly generated instead of using conventional means of identifying phones or their owners, and they may be changed at regular intervals. Cryptographic keys may be used to secure transmissions and geolocation data need not be collected. In addition, the collection of data or metadata by central server authorities that could allow reconstruction of a phone or individual's identity could be prohibited.

[3] See, *e.g.,* "Analysis of DP3T, Between Scylla and Charybdis," Serge Vaudenay, IACR eprint 2020/399 or "Le traçage anonyme, dangereux oxymore," Xavier Bonnetain et al., risques-tracage.fr (in French).

- *The accuracy of contact tracing apps has not been proven and cannot be assumed for multiple technical reasons.* Specifically, Bluetooth technology was not designed to measure distances between devices, cannot recognize when connected devices are separated by a wall or other airflow barrier, and may not register nearby devices, depending upon several factors.[4] Bluetooth-based contact tracing thus appears likely to over-report contacts, and generate a large number of false positives; and

- *High technical quality and functionality will not alone suffice for contact tracing technology to be effective*. Many millions of persons must install an application so the system registers a significant fraction of all interpersonal contacts.[5] Public trust that personal data and privacy will be protected is thus an essential prerequisite for the success of any technologically enabled infection tracking and control program. Accordingly, legal and/or regulatory measures that provide robust safeguards—and are widely understood by the public to do so—must be put in place.

As a body of technical experts, Europe TPC takes no position as to whether or when — from medical, social, political and economic perspectives — contact tracing technology should be deployed in Europe given the technological and social realities identified above. Rather, we provide relevant technical information that will allow policy makers to ***conduct careful risk- and cost-benefit analyses of the consequences of widely deploying an untested technology in novel circumstances before making such determinations***.[6]

Should governments opt to utilize these systems however, we call upon them to use only those which, by technical and legal design:

- respect and protect the rights of all individuals;
- safeguard personal data and privacy to the highest degree technically possible; and
- are subject to scrutiny by the scientific community and civil society before, during and after deployment.

Toward these ends, the ACM Europe Technology Policy Committee urges that the attached principles and practices — addressing architecture, transparency, oversight, safeguards, and public input — be rigorously applied in the development and deployment of any contact tracing technology that might be utilized during the COVID-19 pandemic in the interests of technical efficacy, public trust and public health.

---

[4] See, *e.g.*, GitHub Open Trace Calibration forum analysis.

[5] See, *e.g.*, Science: Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing and The Lancet: Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts.

[6] With regard to risk assessment, we have noted security vulnerabilities inherent in Bluetooth technology. It thus may be expected that organized criminal enterprises will seek to take advantage of new and "always on" Bluetooth activation on millions of smart phones across Europe. (This has not been a serious problem until now as most people use it only for a limited time or in controlled situations, such as their homes or cars.) Regarding costs, we note that Belgium has given up on deploying a contact tracing app for the moment (*see* Lire Coronavirus: la Belgique renonce à une application de traçage des malades) and Valencia has experimented with "citizen-based tracing" (*see* POLITICO - EU Confidential (April 25, 2020)).

Europe Technology Policy Committee

Association for Computing Machinery
acmpo@acm.org | @acmpolicy
www.acm.org/public-policy/europe-tpc

ESSENTIAL CONTACT TRACING APPLICATION PRINCIPLES AND PRACTICES

Technical Architecture

- Cross-border interoperability must be a required technical capacity of any contact tracing technology design and deployment in order to both facilitate international travel and (as many travelers who contract the virus will show symptoms only after they return home) the detection of international infection spread;
- All contact tracing applications, even after download, should be built to require an individual to "opt-in" to the app's activation and to allow its deactivation/reactivation;
- Once volitionally activated, all contact tracing apps must be designed to clearly also require the user to consent to sharing personal information, including any declaration that the user has been infected or deemed by authorities to have been exposed to infection; and
- All sensitive personal information, including infection and exposure status, must not be retained on an individual's device or, if stored, must be password-protected and encrypted.

Development Transparency

- All application and server source code, not only underlying protocols, must be made public;
- Source code must be open to the scrutiny of experts during the entire development process, not merely after a system is ready to be deployed;
- All aspects of the processes by which specific contact tracing technology is solicited and procured, including robust data concerning any individual or corporate technology supplier selected, must promptly be made public; and
- Actual or perceivable conflicts of interest by any individual, entity or consortium developing a contact tracing technology (or one adaptable to that purpose) must promptly be prominently and publicly disclosed.

Expert Oversight

- An independent scientific committee should be established in each country (or each group of countries fully acting in concert) where deployment of contact tracing technology is being considered to technically inform its development, advise policy makers on its likely technical performance and social impacts, provide post-deployment assessments of the technology's effectiveness to policy makers and the public, and offer recommendations regarding its eventual deactivation;
- The proceedings of all such committees should be fully transparent to the public, recorded, and permanently stored in a manner easy for the public to access and research;
- Such committees should be comprised of experts in:
    - technical disciplines (*e.g.*, cryptography, distributed systems, data management, user interface and experience) to ensure that best-in-class algorithms and practices are used in system development, including particularly "privacy by design" and "security by design" principles;
    - social science fields to maximize the acceptability of proposed app designs by the population at large, and such apps' potential impact on social relations, including particularly the potential for digital exclusion, discrimination, stigmatization; and
    - legal matters to ensure compliance with applicable laws and regulations (*e.g.*, GDPR).

Legal Safeguards

- Robust safeguards governing the use of contact tracing technology must be adopted before such technology is deployed and be applicable to all national or multi-national governments, public authorities, and private entities managing such technology. These should, at minimum, include clear statutory or other requirements that:
    - Use of the technical infrastructure is authorized only for the purpose of electronic contact tracing related to fighting the COVID-19 pandemic, and all other uses are explicitly prohibited;
    - Data collected by authorized contact tracing apps may be stored only for as long as is necessary to process that data, and expressly not for any other purpose;
    - No individual shall be required to install, activate, use, or declare or reveal the status of any contact tracing application;
    - No individual, entity of any kind, or governmental body shall be permitted, under penalty of law, to use any technology designed to monitor the installation or use of any contact tracing application;
    - Authorized COVID-19 contact tracing systems will be promptly deactivated when global public health bodies reach consensus that the pandemic is over (*e.g.*, when reliably effective therapies and/or vaccines become widely available); and
    - Such systems also must be shut down promptly if assessed to be ineffective by expert oversight bodies (*e.g.*, because insufficiently adopted, registering an unacceptable level of false positives, or incompatible in practice with fundamental civil liberties).

Public and Civil Society Engagement

- Established national and pan-national mechanisms should be employed for seeking the public's and civil society representatives' comment on proposed contact tracing technology and all aspects of its intended deployment (recognizing that such procedures may need to permit expedited action);
- At minimum, such processes should invite comment on and formally address:
    - fundamental individual rights to privacy at the cornerstone of European democracies;
    - how best to communicate to the public concerning contact tracing apps and their deployment so as to maximize their effectiveness by fostering a sense of common purpose; and
    - the best means of assessing and mitigating the "digital divide" and other potentially exclusionary or discriminatory effects of such technology on all population groups, especially the most vulnerable.

5 May 2020

The Association for Computing Machinery (ACM) is the world's largest and longest established professional society of individuals involved in all aspects of computing. Its Europe Technology Policy Committee promotes sound public policy and public understanding of a broad range of issues at the intersection of technology and policy.

Principal member authors of this document for ACM's Europe Technology Policy Committee are: Michel Beaudouin-Lafon, Enrico Nardelli, and Gerhard Schimpf. Member contributors also include: Panagiota Fatourou, Mario Fritz, Fabrizio Gagliardi, Oliver Grau, and Chris Hankin.