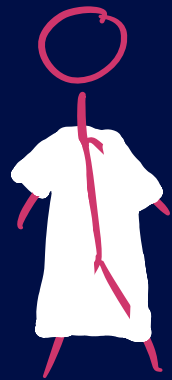


ARE THEY

STUPID, EVIL, OR BOTH?

UNDERSTANDING THE SMITTESTOPP CONFLICT



HANS HEUM
SIMULA U.B



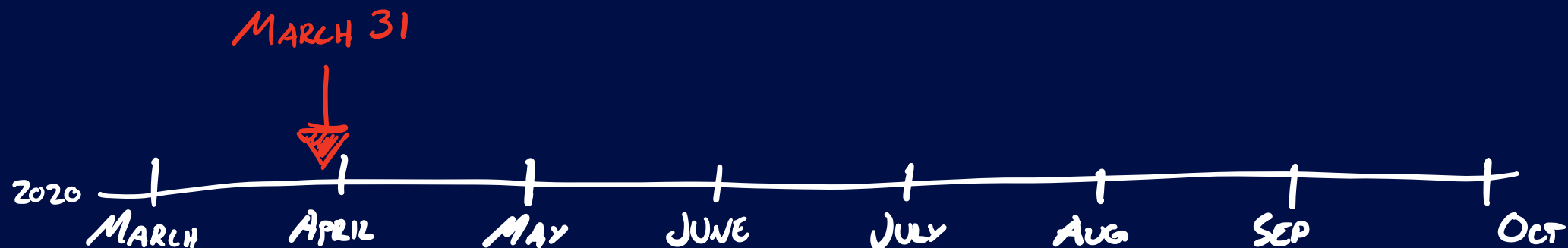
DIGITAL CONTACT TRACING

SCIENCE #368:

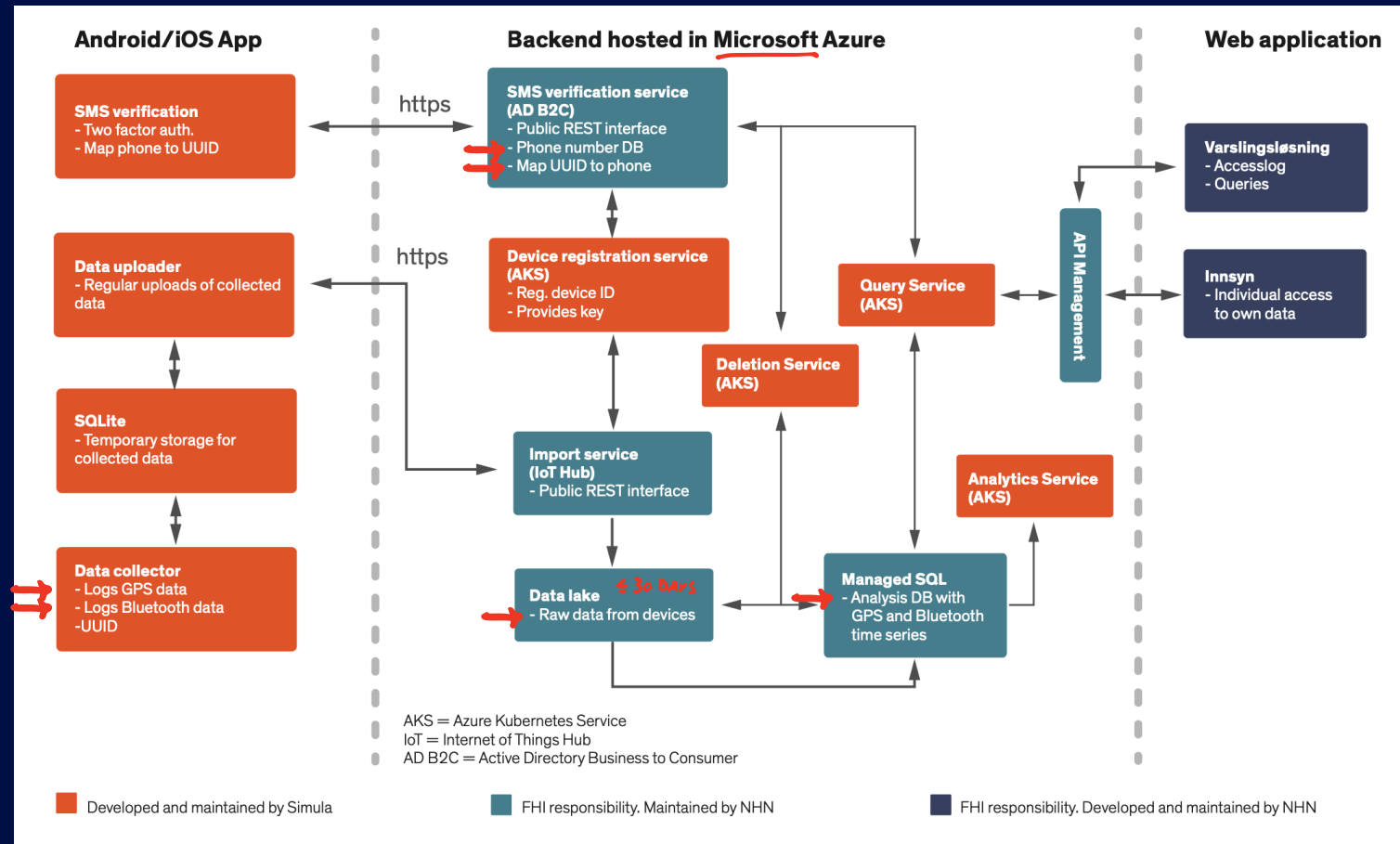
CORONAVIRUS

Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing

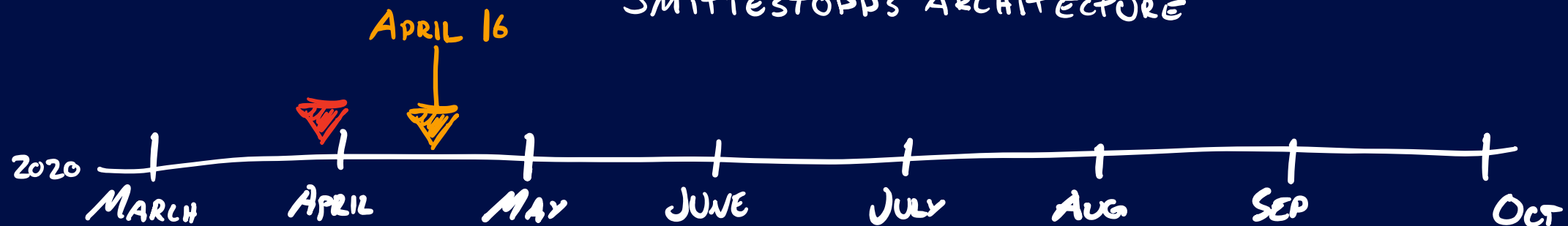
Luca Ferretti*, Chris Wymant*, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall†, Christophe Fraser†‡



NORWAY'S SOLUTION: SMITTESTOPP



SMITTESTOPP'S ARCHITECTURE



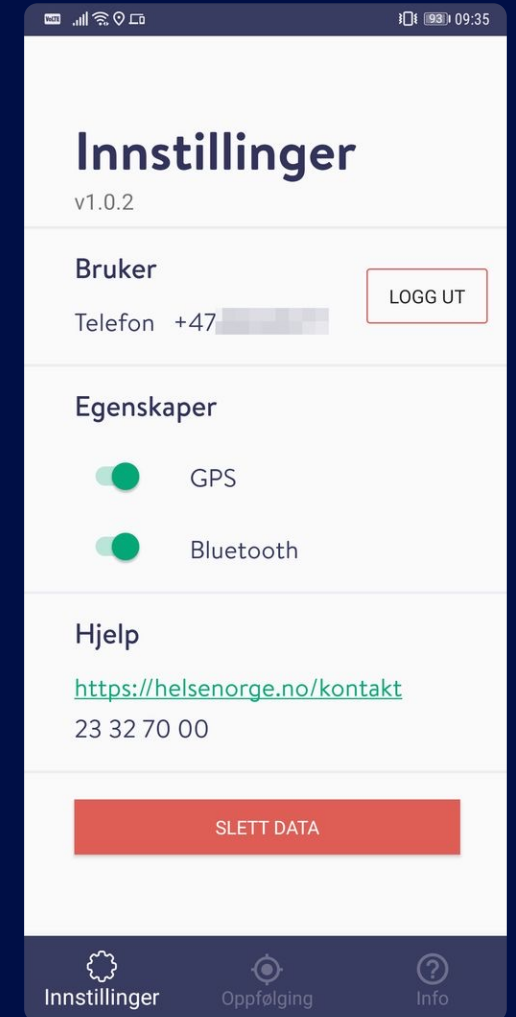
SMITTESTOPP'S USER EXPERIENCE



LONG PRIVACY POLICY STATEMENT

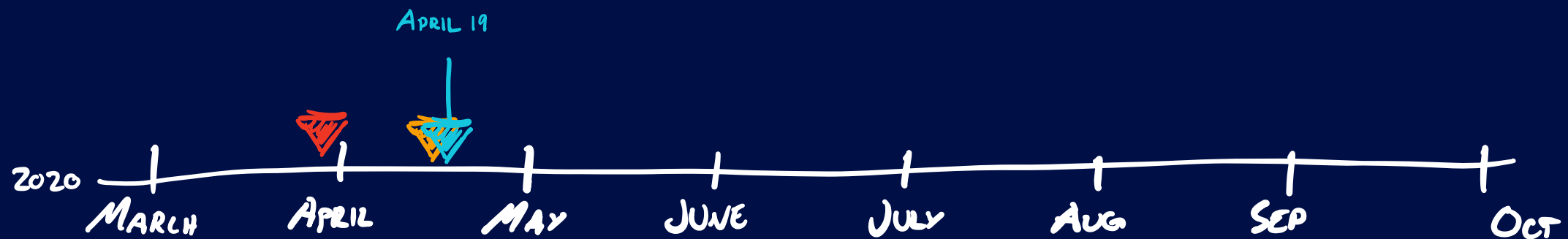


"ALWAYS ALLOWED" NEEDED TO FUNCTION PROPERLY.



JOINT STATEMENT :

- "FULL TRANSPARENCY
IS REQUIRED..."
- "...FOR PROTOCOL AND PROCESSING."

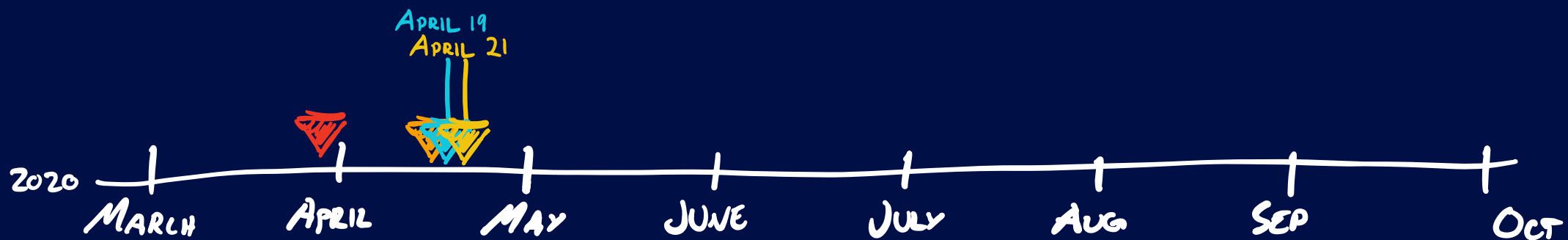


JOINT STATEMENT :

- "FULL TRANSPARENCY IS REQUIRED..."
- "...FOR PROTOCOL AND PROCESSING."

EDPB:

- "DO NOT TRACK THE LOCATION OF USERS."
- "COLLECTED INFORMATION SHOULD RESIDE WITH THE USER."
- "OPERATIONS NOT STRICTLY NECESSARY REQUIRE EXPLICIT CONSENT."



JOINT STATEMENT :

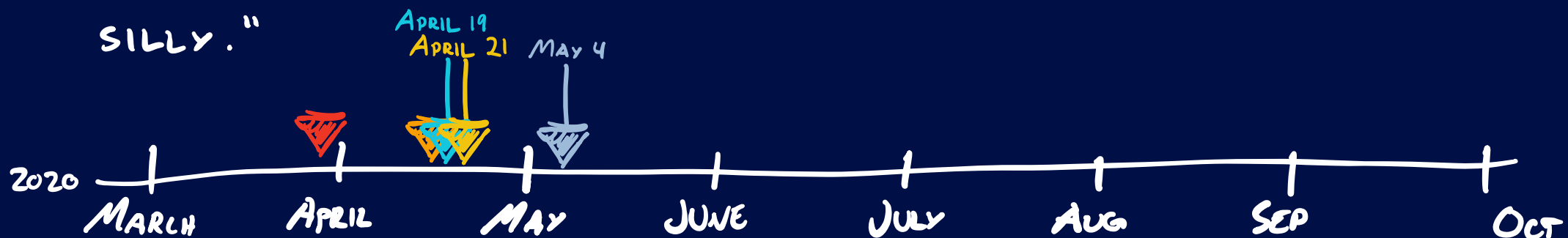
- "FULL TRANSPARENCY IS REQUIRED..."
- "...FOR PROTOCOL AND PROCESSING."

EDPB:

- "DO NOT TRACK THE LOCATION OF USERS."
- "COLLECTED INFORMATION SHOULD RESIDE WITH THE USER."
- "OPERATIONS NOT STRICTLY NECESSARY REQUIRE EXPLICIT CONSENT."

NCSC:

- "USING STATIC IDs WOULD BE SILLY."



JOINT STATEMENT :

- "FULL TRANSPARENCY IS REQUIRED..."
- "...FOR PROTOCOL AND PROCESSING."

EDPB :

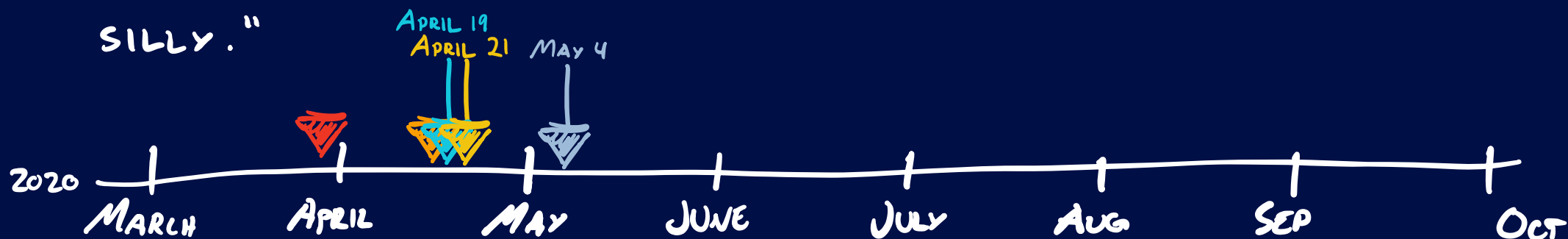
- "DO NOT TRACK THE LOCATION OF USERS."
- "COLLECTED INFORMATION SHOULD RESIDE WITH THE USER."
- "OPERATIONS NOT STRICTLY NECESSARY REQUIRE EXPLICIT CONSENT."

NCSC :

- "USING STATIC IDS WOULD BE SILLY."

SMITTESTOPP :

- CLOSED SOURCE CODE.
- UNCLEAR DATA AGGREGATION METHOD.
- COLLECTED POSITION DATA, (FOR RESEARCH PURPOSES).
- STORED ALL DATA CENTRALLY, (IN IRELAND, SERVERS OPERATED BY MICROSOFT).
- ALL-OR-NOTHING USER AGREEMENT.
- USED STATIC IDS.



REACTIONS TO SMITTESTOPP

Lektor sendte e-post til
høyskoleelever: Omtalte
Smittestopp-appen som
«farligere» enn coronaviruset

VG, APRIL 20



REACTIONS TO SMITTESTOPP

Lektor sendte e-post til
høyskoleelever: Omtalte
Smittestopp-appen som
«farligere» enn coronaviruset

VG, APRIL 20

AMNESTY INTERNATIONAL, JUNE 2:

Given the grave privacy risks to thousands of people, we wanted to alert you to this and urge you to immediately roll back the app in its current form and ensure that any contact tracing efforts are human rights respecting.

Due to the scale of privacy concerns to all users of the app, we plan to make our findings public as soon as possible. We therefore await your response by close of business on 9 June 2020.

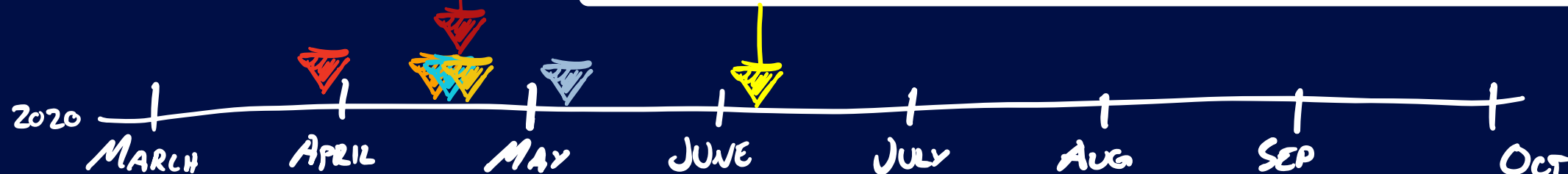
Yours sincerely,



Tanya O'Carroll
Director, Amnesty Tech



John Peder Egenæs
Director, Amnesty International in Norway



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varsler herved følgende vedtak:

Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varsler herved følgende vedtak:

Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.

FHI, JUNE 15:

FHI stopper all innsamling av data i Smittestopp (arkivert)

Publisert 15.06.2020

FHI sletter alle data fra appen Smittestopp og stopper inntil videre innsamling av data etter varsel om forbud fra Datatilsynet. Dette vil gi dårligere beredskap fordi vi taper tid til utvikling og testing av appen, og også dårligere kontroll over smittespredningen i Norge, sier direktør Camilla Stoltenberg.



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varsler herved følgende vedtak:

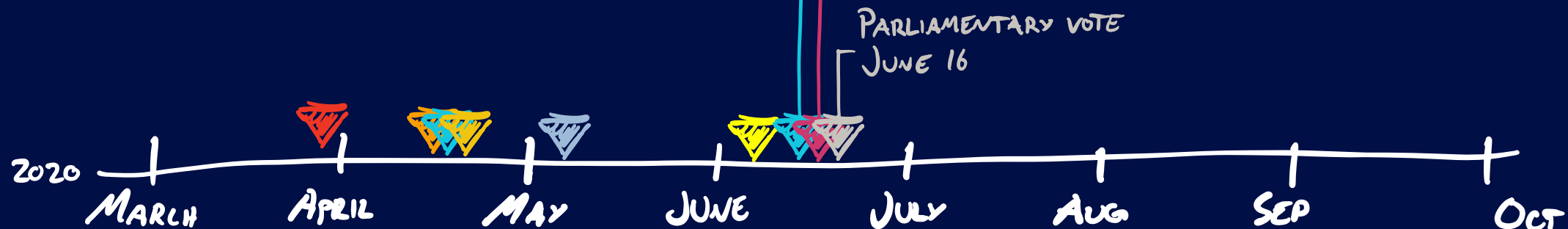
Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.

FHI, JUNE 15:

FHI stopper all innsamling av data i Smittestopp (arkivert)

Publisert 15.06.2020

FHI sletter alle data fra appen Smittestopp og stopper inntil videre innsamling av data etter varsel om forbud fra Datatilsynet. Dette vil gi dårligere beredskap fordi vi taper tid til utvikling og testing av appen, og også dårligere kontroll over smittespredningen i Norge, sier direktør Camilla Stoltenberg.



WHAT THE DEVELOPERS SAID

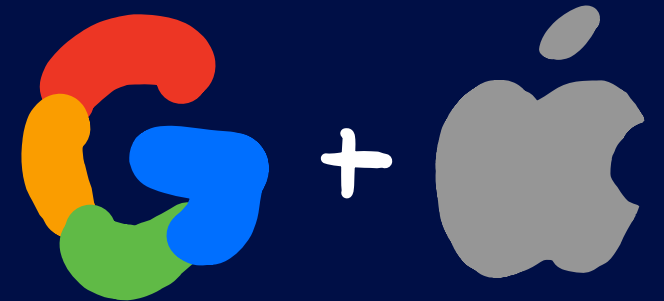
- "SOLVES THE IPHONE PROBLEM"
- "DESIGNED FOR DUAL PURPOSES" (AS PER NIPD'S REQUIREMENTS)
- "CENTRALIZED VS. DECENTRALIZED STILL UNSETTLED"
- "GOOGLE COLLECTS DATA TOO!"

ALL TRUE STATEMENTS, BUT...

THE GOOGLE AND APPLE EXPOSURE NOTIFICATION SYSTEM or, GAEN.

- ONLY DECENTRALIZED SOLUTION TO THE IPHONE PROBLEM.
- GOVERNMENTS HAVE PLEADED APPLE TO LIFT RESTRICTIONS.
- MICHAEL VEALE :

"GAEN IS GREAT FOR INDIVIDUAL PRIVACY,
BUT THE KIND OF INFRASTRUCTURAL POWER IT
ENABLES SHOULD GIVE US SLEEPLESS NIGHTS."



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varslar herved følgende vedtak:

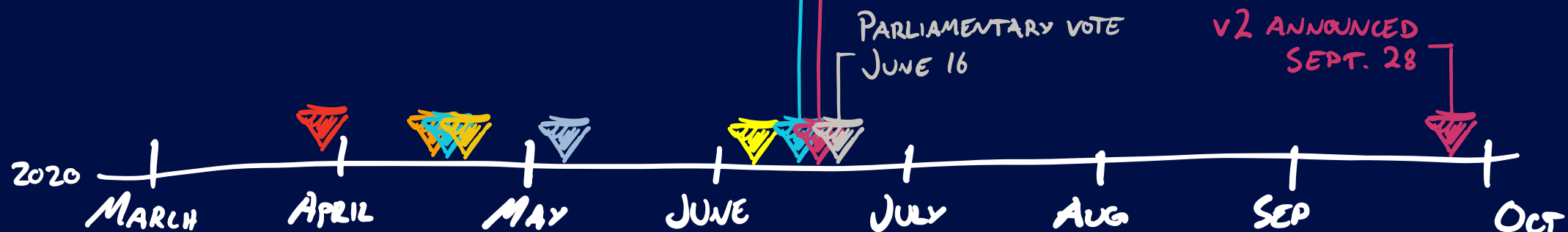
Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.

FHI, JUNE 15:

FHI stopper all innsamling av data i Smittestopp (arkivert)

Publisert 15.06.2020

FHI sletter alle data fra appen Smittestopp og stopper inntil videre innsamling av data etter varsel om forbud fra Datatilsynet. Dette vil gi dårligere beredskap fordi vi taper tid til utvikling og testing av appen, og også dårligere kontroll over smittespredningen i Norge, sier direktør Camilla Stoltenberg.



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varslar herved følgende vedtak:

Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.

FHI, JUNE 15:

FHI stopper all innsamling av data i Smittestopp (arkivert)

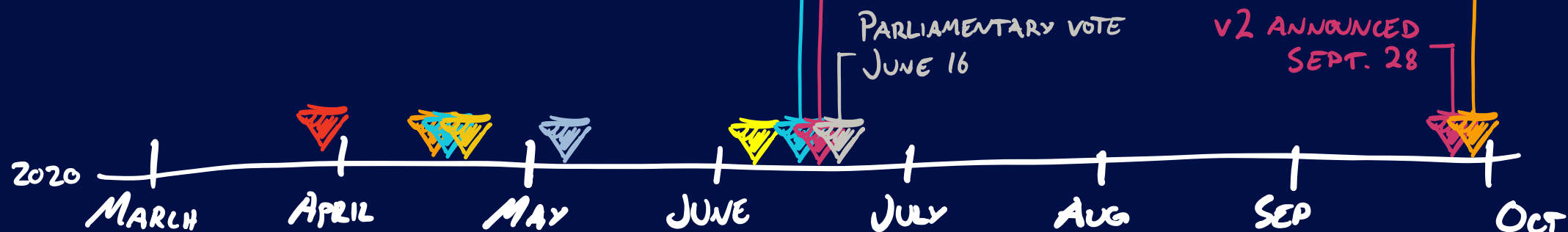
Publisert 15.06.2020

FHI sletter alle data fra appen Smittestopp og stopper inntil videre innsamling av data etter varsel om forbud fra Datatilsynet. Dette vil gi dårligere beredskap fordi vi taper tid til utvikling og testing av appen, og også dårligere kontroll over smittespredningen i Norge, sier direktør Camilla Stoltenberg.

DIGI.NO, SEPT. 29:

SIMULAS SMITTESTOPP

Simula langer ut: – Rapporten Amnesty har levert er direkte søppel, og er et stykke elendig arbeid



THE END OF SMITTESTOPP (v1)

DATATILSYNET, JUNE 12:

8. Varsel om vedtak

Datatilsynet varslar herved følgende vedtak:

Folkehelseinstituttet ilegges et midlertidig forbud mot å behandle personopplysninger knyttet til Smittestopp, jf. personvernforordningen artikkel 58 nr. 2 bokstav f.

FHI, JUNE 15:

FHI stopper all innsamling av data i Smittestopp (arkivert)

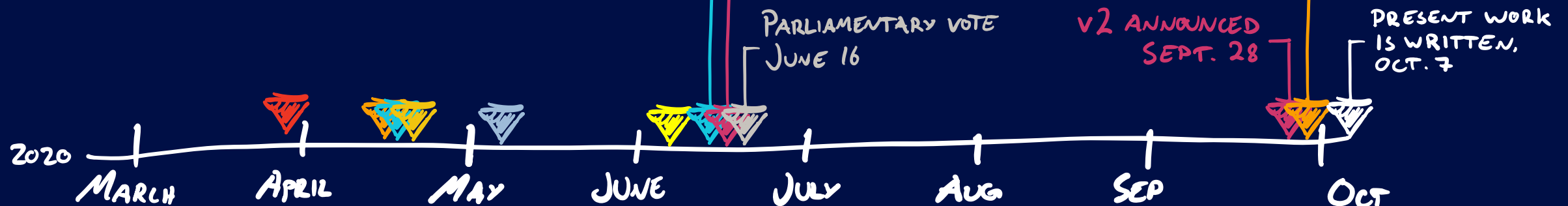
Publisert 15.06.2020

FHI sletter alle data fra appen Smittestopp og stopper inntil videre innsamling av data etter varsel om forbud fra Datatilsynet. Dette vil gi dårligere beredskap fordi vi taper tid til utvikling og testing av appen, og også dårligere kontroll over smittespredningen i Norge, sier direktør Camilla Stoltenberg.

DIGI.NO, SEPT. 29:

SIMULAS SMITTESTOPP

Simula langer ut: – Rapporten Amnesty har levert er direkte søppel, og er et stykke elendig arbeid



FAST FORWARD 1 YEAR...

NATURE COMMUNICATIONS, OCT 11, 2021

ARTICLE

 Check for updates

<https://doi.org/10.1038/s41467-021-26144-8>

OPEN

Nationwide rollout reveals efficacy of epidemic control through digital contact tracing

Ahmed Elmokashfi^{1✉}, Joakim Sundnes², Amund Kvalbein¹, Valeriya Naumova¹, Sven-Arne Reinemo¹, Per Magne Florvaag², Håkon Kvale Stensland^{2,3} & Olav Lysne^{1,4}

Fuelled by epidemiological studies of SARS-CoV-2, contact tracing by mobile phones has been put to use in many countries. Over a year into the pandemic, we lack conclusive evidence on its effectiveness. To address this gap, we used a unique real world contact data set, collected during the rollout of the first Norwegian contact tracing app in the Spring of 2020. Our dataset involves millions of contacts between 12.5% of the adult population, which enabled us to measure the real-world app performance. The technological tracing efficacy was measured at 80%, and we estimated that at least 11.0% of the discovered close contacts could not have been identified by manual contact tracing. Our results also indicated that digital contact tracing can flag individuals with excessive contacts, which can help contain superspreading related outbreaks. The overall effectiveness of digital tracing depends strongly on app uptake, but significant impact can be achieved for moderate uptake numbers. Used as a supplement to manual tracing and other measures, digital tracing can be instrumental in controlling the pandemic. Our findings can thus help informing public health policies in the coming months.



THE DATASET

- DAILY "PSEUDONYMIZED" AGGREGATES...
- ... ON A PER-USER BASIS.
- COLLECTED FROM APRIL 17 – JUNE 4 2020.
- 545 354 DEVICES ; 26 792 433 DEVICE-TO-DEVICE CONTACTS.
- BLUETOOTH DATA ONLY.
- OBTAINED FROM FHI WITH PERMISSION OF USE.
- FULL DATASET AVAILABLE UPON REQUEST.

	All	PC	RRC	PRC
Unique devices	545354	525646	485730	461068
Unique contacts	26792433	10665399	3946986	2889922

FROM SUPP. NOTE 2: "DATASET"

THE LEGAL STATEMENT

FROM SUPP. NOTE 10, "LEGALITY OF THE DATASET":

The law firm Wiersholm concludes that the data-set can be legally used for research purposes if there does not exist additional information that would make it possible to re-identify persons under the assumption that all reasonable means for re-identification is used. NSD writes that it is hard to imagine how a motivated intruder can successfully re-identify anyone, given that the data in the set is not part of any other registries. Simula Research Laboratory therefore conclude that use of the data-set for research purposes is legal.

FROM "JOINT STATEMENT ON CONTACT TRACING" (APRIL 2020)

- The use of contact tracing Apps and the systems that support them must be voluntary, used with the explicit consent of the user and the systems must be designed to be able to be switched off, and all data deleted, when the current crisis is over.

ArXiv 2112.03839

NISK 2021

Stupid, Evil, or Both? Understanding the Smittestopp conflict

Hans Heum¹

Simula UiB
Merkantilen (3rd floor)
Thormøhlensgate 53D
N-5006 Bergen, Norway.
hansh@simula.no

Abstract. Like many governments, the Norwegian government provided a contact tracing application to help in combating the COVID-19 pandemic at its outset. However, the application was widely criticized for enabling an unacceptable intrusion into its subjects' lives, leading to its discontinuation only four months into the pandemic. In this essay, we will take a closer look at what went wrong, attempt to gain a deeper understanding of the passionate nature of the conflict, and how both sides came to view the other as being either stupid, or evil, or both.¹

Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

Tjerand Silde¹  and Martin Strand² 

¹ Department of Mathematical Sciences
Norwegian University of Science and Technology – NTNU
tjerand.silde@ntnu.no

² Norwegian Defence Research Establishment – FFI
martin.strand@ffi.no

eprint 2021/203

Abstract. Anonymous single-use tokens have seen recent applications in private Internet browsing and anonymous statistics collection. We develop new schemes in order to include public metadata such as expiration dates for tokens. This inclusion enables planned mass revocation of tokens without distributing new keys, which for natural instantiations can give 77 % and 90 % amortized traffic savings compared to Privacy Pass (Davidson *et al.*, 2018) and DIT: De-Identified Authenticated Telemetry at Scale (Huang *et al.*, 2021), respectively. By transforming the public key, we are able to append public metadata to several existing protocols essentially without increasing computation or communication. Additional contributions include expanded definitions, a more complete framework for anonymous single-use tokens and a description of how anonymous tokens can improve the privacy in dp³t-like digital contact tracing applications. We also extend the protocol to create efficient and conceptually simple tokens with both public and private metadata, and tokens with public metadata and public verifiability from pairings.

NISK 2022

Attack vectors to re-identify individuals from the anonymised Smittestopp dataset

Hagen Echzell

Independent Researcher
Oslo, Norway
hagen.pub@echzell.org

Abstract. The first version of “Smittestopp”, the Norwegian Institute of Public Health’s (NIPH) contact tracing application, centrally stored data about the population’s contact patterns with reference to a static personal identifier, a decision that has been widely discussed and criticised. After the Norwegian Data Protection Authority had temporarily forbidden further data collection and processing in June 2020, NIPH announced to discontinue the app and stated that all data related to the application would be deleted. Nevertheless, in October 2021, researchers from an institution involved in the development of the app published a paper called “Nationwide rollout reveals efficacy of epidemic control through digital contact tracing” [3]. In their paper, they analysed a derived dataset based on the Smittestopp data that was announced to be deleted. The authors claim that this derived dataset was anonymised and therefore does not include any personal data. We challenge this assumption by explaining how different external sets of personal data can be matched with the dataset, which potentially leads to a re-identification of persons and a disclosure of their private contacts. We conceptually show how some of these methods can be applied on an example case using publicly available information on Erna Solberg, Norway’s former prime minister. We conclude that it appears reasonably likely that individuals can be re-identified and that the dataset should not be considered anonymised.

NTNU.No / ...

ArXiv 2112.03839

NISK 2021

Stupid, Evil, or Both? Understanding the Smittestopp conflict

Hans Heum¹

Simula UiB
Merkantilen (3rd floor)
Thormøhlensgate 53D
N-5006 Bergen, Norway.
hansh@simula.no

Abstract. Like many governments, the Norwegian government provided a contact tracing application to help in combating the COVID-19 pandemic at its outset. However, the application was widely criticized for enabling an unacceptable intrusion into its subjects' lives, leading to its discontinuation only four months into the pandemic. In this essay, we will take a closer look at what went wrong, attempt to gain a deeper understanding of the passionate nature of the conflict, and how both sides came to view the other as being either stupid, or evil, or both.¹

Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

Tjerand Silde¹  and Martin Strand² 

¹ Department of Mathematical Sciences
Norwegian University of Science and Technology – NTNU
tjerand.silde@ntnu.no

² Norwegian Defence Research Establishment – FFI
martin.strand@ffi.no

eprint 2021/203

Abstract. Anonymous single-use tokens have seen recent applications in private Internet browsing and anonymous statistics collection. We develop new schemes in order to include public metadata such as expiration dates for tokens. This inclusion enables planned mass revocation of tokens without distributing new keys, which for natural instantiations can give 77 % and 90 % amortized traffic savings compared to Privacy Pass (Davidson *et al.*, 2018) and DIT: De-Identified Authenticated Telemetry at Scale (Huang *et al.*, 2021), respectively. By transforming the public key, we are able to append public metadata to several existing protocols essentially without increasing computation or communication. Additional contributions include expanded definitions, a more complete framework for anonymous single-use tokens and a description of how anonymous tokens can improve the privacy in dp³t-like digital contact tracing applications. We also extend the protocol to create efficient and conceptually simple tokens with both public and private metadata, and tokens with public metadata and public verifiability from pairings.

NISK 2022

Attack vectors to re-identify individuals from the anonymised Smittestopp dataset

Hagen Echzell

Independent Researcher
Oslo, Norway
hagen.pub@echzell.org

Abstract. The first version of “Smittestopp”, the Norwegian Institute of Public Health’s (NIPH) contact tracing application, centrally stored data about the population’s contact patterns with reference to a static personal identifier, a decision that has been widely discussed and criticised. After the Norwegian Data Protection Authority had temporarily forbidden further data collection and processing in June 2020, NIPH announced to discontinue the app and stated that all data related to the application would be deleted. Nevertheless, in October 2021, researchers from an institution involved in the development of the app published a paper called “Nationwide rollout reveals efficacy of epidemic control through digital contact tracing” [3]. In their paper, they analysed a derived dataset based on the Smittestopp data that was announced to be deleted. The authors claim that this derived dataset was anonymised and therefore does not include any personal data. We challenge this assumption by explaining how different external sets of personal data can be matched with the dataset, which potentially leads to a re-identification of persons and a disclosure of their private contacts. We conceptually show how some of these methods can be applied on an example case using publicly available information on Erna Solberg, Norway’s former prime minister. We conclude that it appears reasonably likely that individuals can be re-identified and that the dataset should not be considered anonymised.

NTNU.No / ...

THANKS!

CODES OF ETHICS AS A TOOL FOR UNDERSTANDING, 1

CAMP 1: THE MEDICAL RESEARCH COMMUNITY

- WHO
- FHI (NIPH)
(WITH SUPPORT FROM SIMULA)

ETHICS:

- HIPPOCRATIC OATH
- "RESEARCH IN GLOBAL HEALTH EMERGENCIES: ETHICAL ISSUES."
- MAIN SAFEGUARDS: COUNCELLING, OVERSIGHT.

NSD

We ensure that data about people and society can be collected, stored and shared, both safely and legally, today and in the future.

(NORSK SENTER FOR FORSKNINGSDATA)



CODES OF ETHICS AS A TOOL FOR UNDERSTANDING, 2

CAMP 2: THE PRIVACY COMMUNITY

- ENGINEERS AND HOBBYISTS
- DATATILSYNET (NDPA)
- AMNESTY INTERNATIONAL



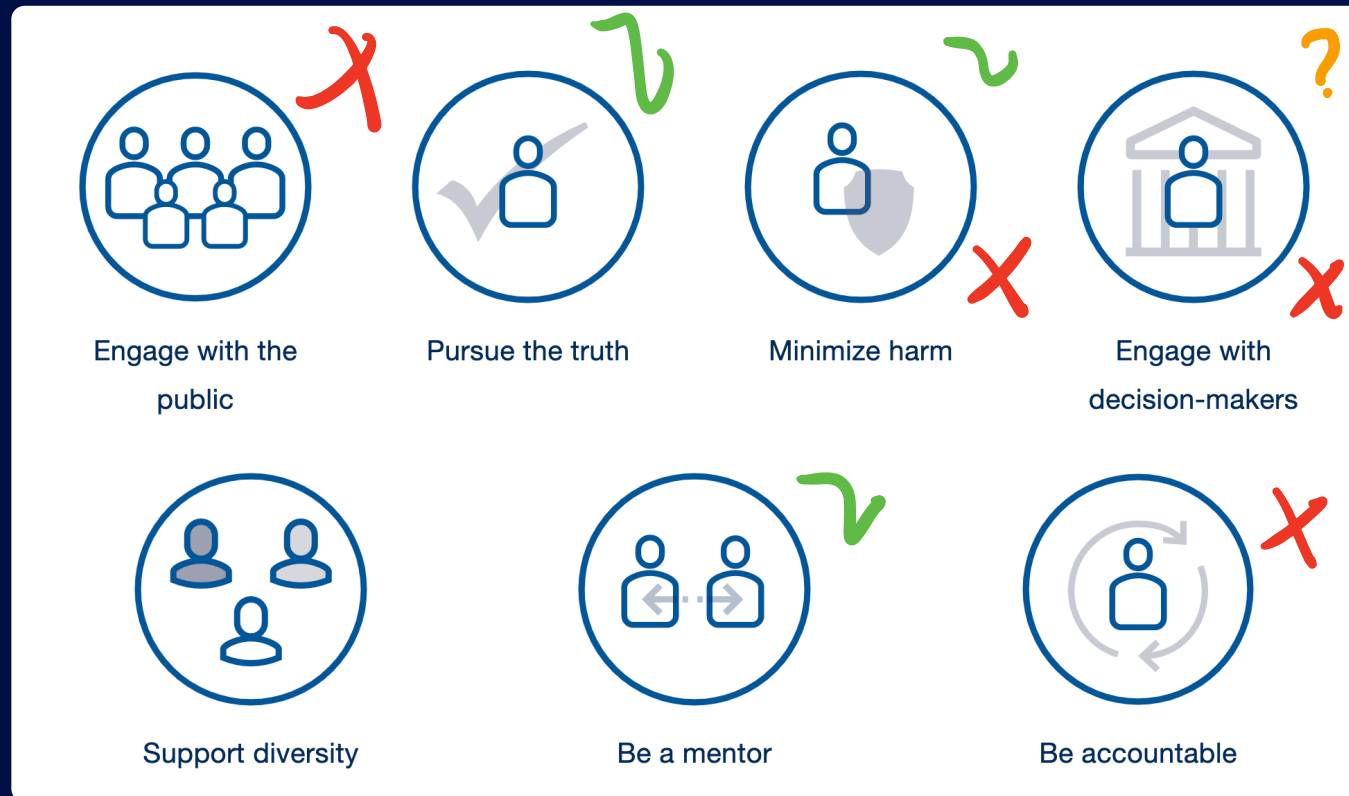
RICHARD STALLMAN IN XKCD # 344

ETHICS:

- ARTICLE 12 OF THE
UNIVERSAL DECLARATION OF HUMAN RIGHTS
- A CYPHERPUNK'S MANIFESTO (1993)



CONCLUSION: A COMMON CODE OF ETHICS



"A CODE OF ETHICS
FOR RESEARCHERS",
THE WORLD ECONOMIC
FORUM, 2018.

CONTACT: HANSH@SIMULA.NO