POLITIET
POLITIDIREKTORATET

Morphing Attack Detection Capabilities of Human Examiners

Frøy Løvåsdal

Senior Adviser

National Police Directorate, Norway

POLITIET
POLITIDIREKTORATET

Frøy

- 24 years working for the Norwegian Government
- Ministry of Foreign Affairs, Directorate of Immigration, Norwegian ID Centre, National Police Directorate, Norway
- Technology, innovation, identity, immigration, passports, citizenships, anti-fraud, anti-human trafficking, Schengen co-operation, consular affairs, media, management, project management…
- System development, projects to improve quality, security and efficiency
- Biometrics 12 years
- Forensic Facial Examiner 5 years
- Now: Biometrics at the ID Section, Team Leader – Identity Strategy, EUIS Programme

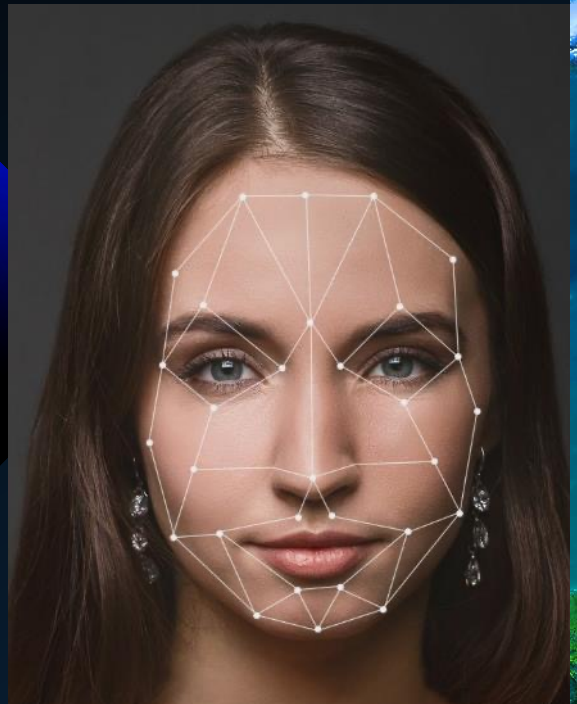
Acknowledgement (and Disclaimer)

– The iMARS-Project has received funding from the European Union's H2020 research and innovation programme under grant agreement No 883356

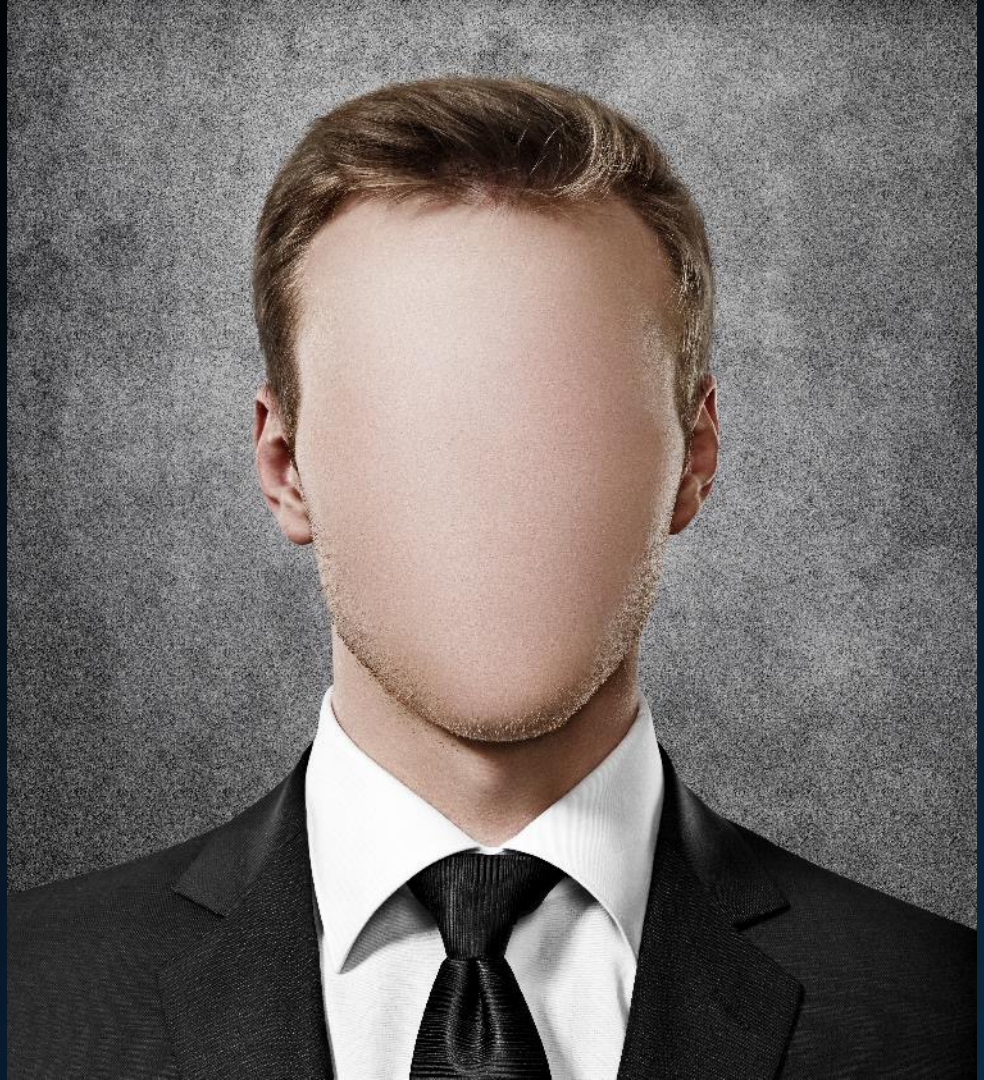
– The content of this presentation represents the views of the author only and is her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

POLITIET
POLITIDIREKTORATET

One person – One Identity – In Norway



POLITIET
POLITIDIREKTORATET



POLITIET
POLITIDIREKTORATET

Biometrics - ISO/IEC 2382-37

*"**automated** recognition of individuals based on their biological and behavioural characteristics"*

- I.e. a process carried out by machines
- Biometric comparison

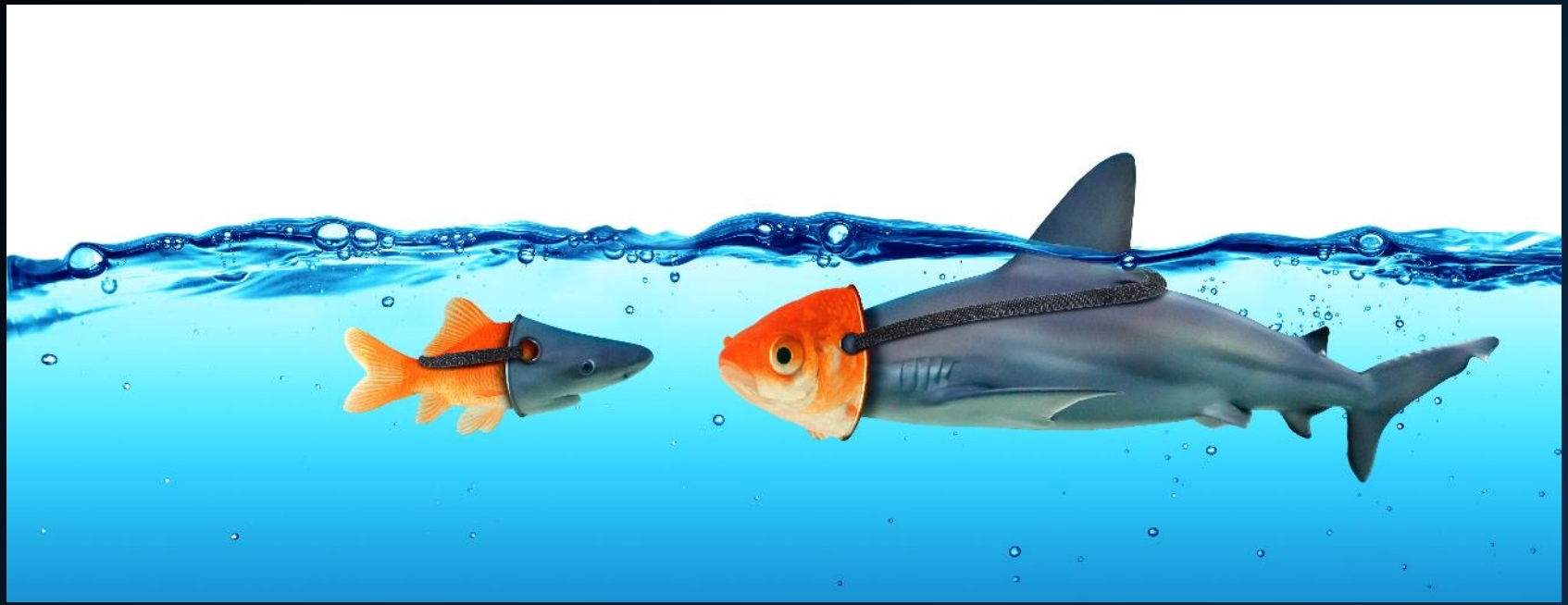
- Facial image, fingerprints, iris image, etc. are **not biometrics**, but biometric data*

- Manual comparison of faces, fingerprints, etc.

* GDPR

POLITIET
POLITIDIREKTORATET

Presentation Attacks



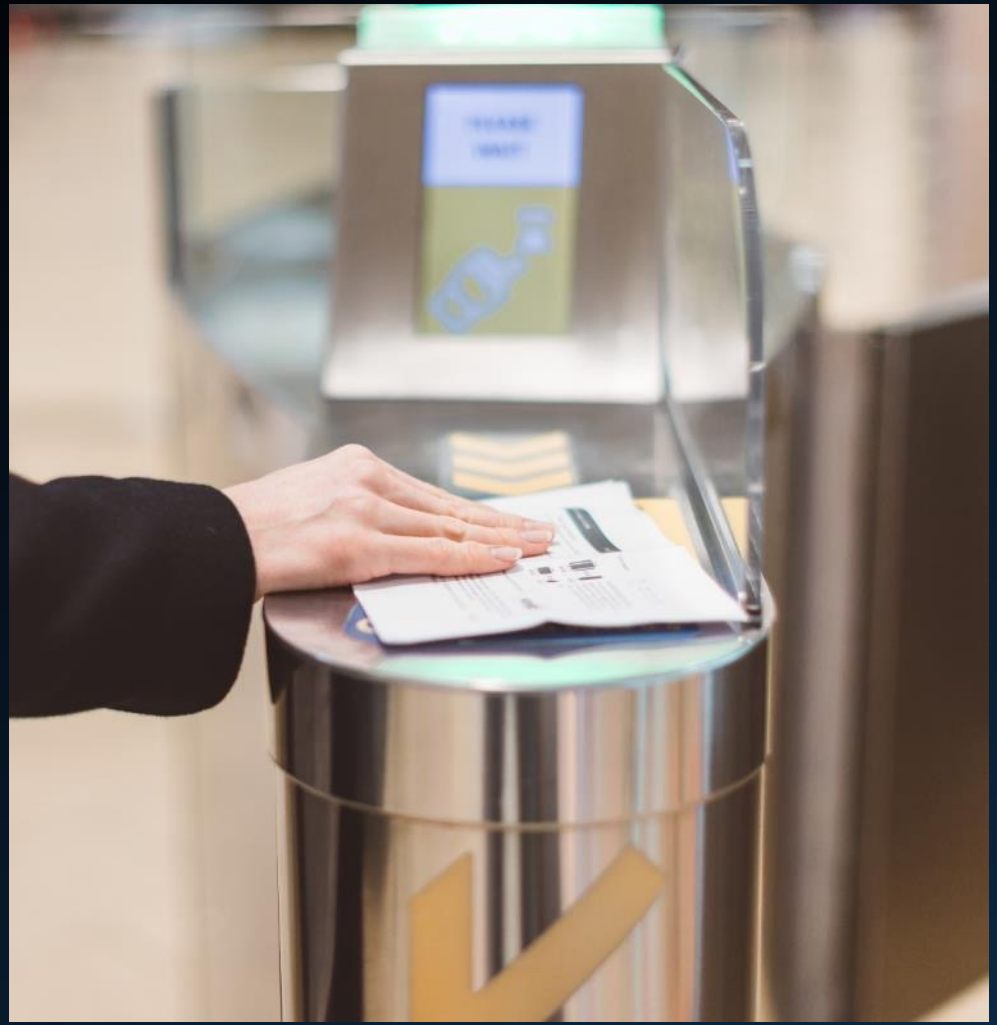
POLITIET
POLITIDIREKTORATET

https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html


SUOMI - FINLAND
Diplomatic Passport
Passeport Diplomatique
DIPLOMAATTILINEN PASS
DIPLOMATIC PASSPORT
SPECIAL PASSPORT
DIPLOMATISKÁ PASE
REPUBLIC OF KOREA
TÜRKİYE CUMHURİ
REPUBLIC OF TURKE
PASAPORT
PASSPORT

POLITIET
POLITIDIREKTORATET



POLITIET
POLITIDIREKTORATET


AUFENTHALTSTITEL
Name
BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

POLITIET
POLITIDIREKTORATET

iMARS

image Manipulation Attack Resolving Solutions

(http://www.imars-project.eu)

POLITIET
POLITIDIREKTORATET

iMARS

- Research Consortium consisting of:
  - 7 universities
    - *4 technical*
    - *3 legal, ethical, societal*
  - 9 countries (Govt.)
    - *Document issuing authorities*
    - *Border Authorities*
    - *Law Enforcement*
  - 6 private industry

POLITIET
POLITIDIREKTORATET

iMARS

- Develop algorithms (PAD/MAD)
  - Morphing
  - Manipulation
- Fraud Detection Tools
- Applicable for:
  - Borders
  - Law enforcement/Forensics
  - Passport issuance

POLITIET
POLITIDIREKTORATET

iMARS

- Develop training
- Databases for testing and training
- Standards development (ISO)
  - PAD
  - Image Quality Assessment

POLITIET
POLITIDIREKTORATET

iMARS

Research activity:

Analysing Human Observer Ability

Norwegian University of Science and Technology

&

National Police Directorate, Norway

Motivation

- Algorithms are great, but humans are part of the mix
- Some years before we have robust algorithms suited for operational scenarios
- Humans are probably not great at this…
- Security concern
- Urgent need for trained staff

Motivation

- How good are people at detecting morphs today?
- How much time is needed to detect a morph?
- How sure can humans get?
- What kind of training is needed? –And how much?
- Individual ability?

POLITIET
POLITIDIREKTORATET

Planned activities

High level plan

- Benchmark ✓
- Super-recognisers
- Annotations, Certainty
- Eye-tracker
- Develop and provide training
- Test
- Amend and provide training
- Test

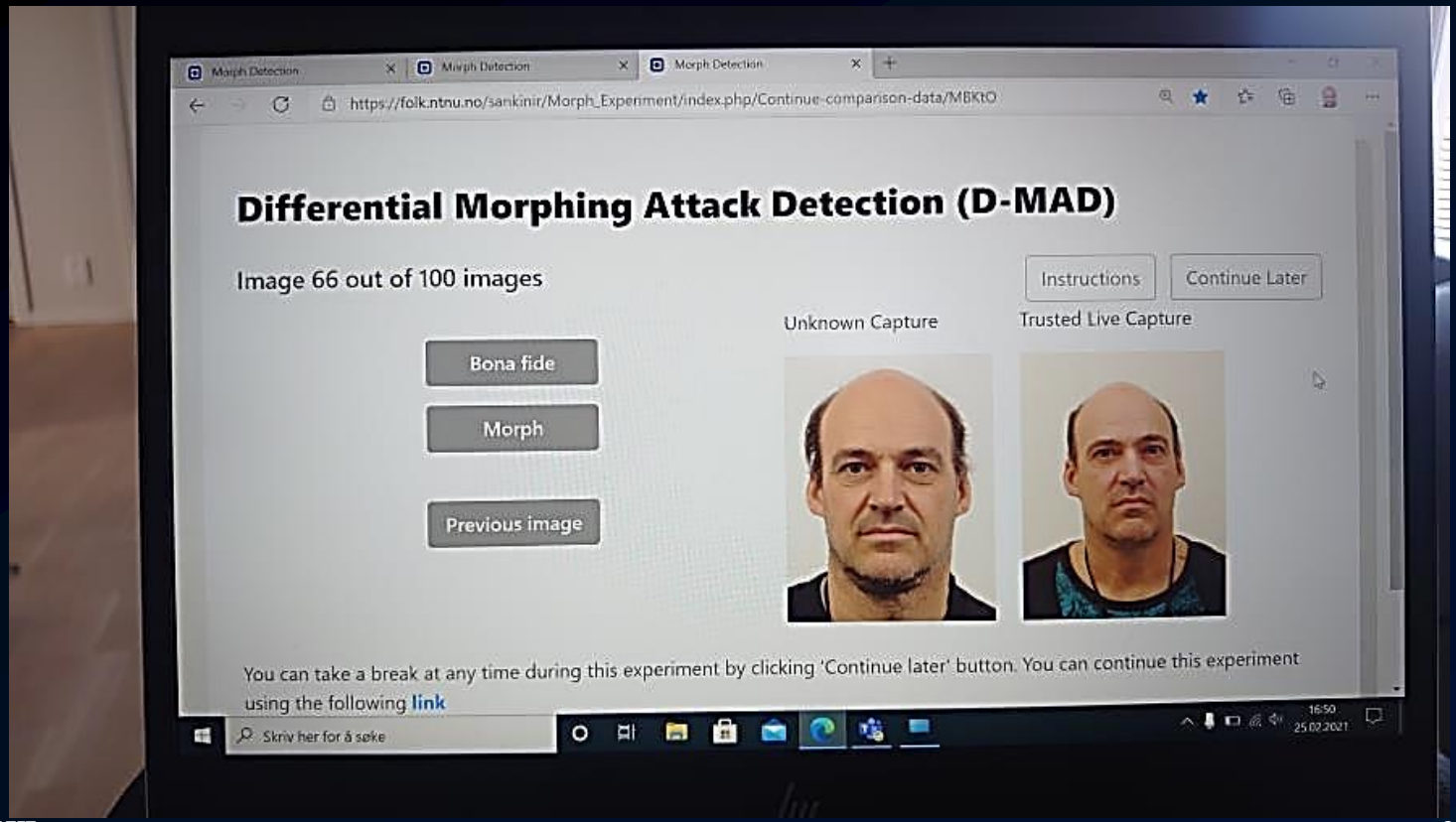
Activity Plan

Part 1: Benchmark

- D-MAD experiment – 400 image pairs
  - One picture of unknown origin (document)
  - One reference picture (e-gate)

- S-MAD experiment – 180 images
  - One picture of unknown origin (document)

Example D-MAD Experiment



Activity Plan

Part 1: Benchmark

- D-MAD experiment – 400 image pairs
  - One picture of unknown origin (document)
  - One reference picture (e-gate)

- S-MAD experiment – 180 images
  - One picture of unknown origin (document)

Activity plan

- Generate training based on:
  - Information gathered in previous experiments
  - Analysis done in the technical track
  - Qualitative research?
- Feed algorithms info from humans (that do well)
- "Explainability"

POLITIET
POLITIDIREKTORATET

Design

Test Platform @ NTNU

- Created by Ms Sankini Rancha Godage
- Supervisor 1: Prof. Dr. Kiran Raja, Norwegian University of Science and Technology (NTNU)
- Supervisor 2: Ms Frøy Løvåsdal, National Police Directorate, Norway

Design

- Invitation to participate (with URLs)
- GDPR compliant consent form (integrated)
- Registration form
- Experiments:
  - D-MAD
  - S-MAD

Registration form

- Email (voluntary)
- Gender, age
- Trained in:
  - Facial Examination? – Time?
  - Document Examination? – Time?
  - Morphing Detection? – Time?
- Super-recogniser? ('Documented')
- Line of work

The Test Databases

- D-MAD - Paid and unpaid volunteers (NTNU)
- S-MAD - FRGC dataset (University of Notre Dame). https://cvrl.nd.edu/projects/data/
- Digital and analogue images
- 1 camera for enrolment
- eGates at NTNU for reference images
- 1 scanner
- 1 printer

The Test Database

- Max two images in each morph
- Two different algorithms
- NTNU – Locating landmarks
- UBO - Morphing
- Post processing by 1 person, checked by 1 other (Adobe Photoshop)

POLITIET
POLITIDIREKTORATET

Results

Participation

Number of participants:

- D-MAD: 469
- S-MAD: 410
- 1 experiment only – 700+ people
- Border guards, case handlers (visas, passports, residence permits, asylum), ID experts, forensic face/fingerprint/document examiners….
- 40+ countries

Control Group (100 people)

- Staff and students at NTNU
- Do people understand the registration form?
- Do people understand what they are supposed to do in the experiments?
- How long does the study take?

Pilot

Summary of results

- Performance vary enormously
- Time spent vary enormously
- Little or no correlation between the two (above)
- MAD Competence seems to improve during experiments

Summary of results

- Untrained staff same performance as 3rd line (forensic) face / document examiners
- Face examiners slightly better than document examiners
- S-MAD harder than D-MAD
- Print-scan – Less of a problem for humans
- High performers everywhere

POLITIET
POLITIDIREKTORATET

Factors potentially affecting the results of the study

Potential errors in the study

- People could lie
- Erroneous registration of one or more field
- Super recogniser – 'Documented'
- Language – Misunderstandings (e.g. SR)
- Score and time info after 100 pairs/tasks

Potential errors in the study

- Participants know they are being tested
  - Spend more time than with a real case
  - Spend less time because it is not a real case
- Fatigue – Experiment in addition to real job
- Restart with new email address

Potential errors in the study

- Time spent – doing other work in between (not stopping experiment when taking breaks…)
  - Follow up activity?
  - Encourage participants to use the 'continue later' button in upcoming experiments?
    - Could add stress and lead to participants contacting admin to correct time

(Additional) Lessons learned

- Lack of knowledge
  - What is morphing?
  - Is it relevant for me/my field?
- Managers: Who participated? Anonymous, but…
  Next time: E.g. categories for
  - Norwegian police
    - District
    - Section
    - Unit

POLITIET
POLITIDIREKTORATET

Preliminary feedback from the participants

Feedback from the participants

- 'Next level'
- 'Fun', 'interesting', 'challenging'
- 'Horrible', 'very difficult', 'self-esteem killing', 'shooting whilst blind-folded', 'no idea what I am doing'
- Prior training not always a positive

POLITIET
POLITIDIREKTORATET

Next steps

High level plan

- Benchmark ✓
- Super-recognisers
- Eye-tracker
- Annotations, Certainty
- Develop and provide training
- Test
- Amend and provide training
- Test

High level plan – Long term

- Certifications at different levels?
  - E.g. 1st , 2nd, 3rd level examination
  - Available time for examination differs depending on line of work

High level plan – Future steps

- Annual / bi-annual proficiency testing?
  - Some agencies may not see many morphs in a year
  - Certification and recent proficiency test results useful for internal quality reviews, risk assessments, future court appearances, etc.
- Testing part of recruitment and selection?

POLITIET
POLITIDIREKTORATET

Summary

- Morphing is a serious security risk
- No good countermeasures
- Morphed passports will be in circulation for many years
- Solving the problem will take years…
- We need human expertise NOW!

Future research (morphing and other type of manipulation)

- Examiners, case handlers, border guards, super-recognisers, etc. wanted!
- By participating you are:
  - Contributing to important research
  - (Hopefully) Improving your own ability to detecting morphed images

Thank you!

POLITIET
POLITIDIREKTORATET

Questions / Participation in future testing and training?

- Frøy Løvåsdal
Senior Adviser
National Police Directorate, Norway

- M: +47 468 86 101
- E: Froy.lovasdal@politiet.no