Thoughtful Biometrics Workshop

March 8, 10 & 12, 2021
Online in @QiqoChat

Book of Proceedings

https://thoughtfulbiometrics.org/

Welcome to the Thoughtful Biometrics Workshop

Monday, Wednesday, Friday / March 8, 10, 12, 2021
9:00am to 2:00pm PST / 12:00pm to 5:00pm EST - Each Day

Thank you to our Founding Sponsors

VERIDIUM TRUSTED DIGITAL IDENTITY acuant accessnow

#TBW2021 is the time and space to dialogue about critical emerging issues surrounding biometric and digital identity technologies. Biometrics technology is being used in a wide range of contexts and within this range of existing and potential uses, there are many questions about ethical and socially good uses.

Image Commentary (creative commons licensed (CC by 2.5)
This image reflects a range of different biometrics modalities. We note that the subject in the image is a white male and this reflects one of the questions about the industry, is it true that biometrics systems are built based on a default human "the white guy"? Does this mean that women and people of color are not included, or that biometric systems are inherently biased? ~ We also note that there is a law enforcement person who is watching and accessing the data, invading the privacy of the individual.

We've chosen this image because it highlights the growing concerns about biometric function creep where biometric data can be shared and misused without users' knowledge via these interconnected biometric systems.

Thoughtful Biometrics Workshop
Co-founded by Kaliya Young, Asem Othman, John Callahan
Co-produced by Heidi Nobantu Saul, Kaliya Young
Co-Facilitated by Kaliya Young, Heidi Nobantu Saul, Dounia Saeme

Contents

Welcome to the Thoughtful Biometrics Workshop

Monday, Wednesday, Friday / March 8, 10, 12, 2021
9:00am to 2:00pm PST / 12:00pm to 5:00pm EST - Each Day

THANK YOU TO OUR FOUNDING SPONSORS

VERIDIUM TRUSTED DIGITAL IDENTITY acuant accessnow

#TBW2021 is the time and space to dialogue about critical emerging issues surrounding biometric and digital identity technologies. Biometrics technology is being used in a wide range of contexts and within this range of existing and potential uses, there are many questions about ethical and socially good uses.

Image Commentary (creative commons licensed (CC by 2.5)

This image reflects a range of different biometrics modalities. We note that the subject in the image is a white male and this reflects one of the questions about the industry, is it true that biometrics systems are built based on a default human "the white guy"?Does this mean that women and people of color are not included,

TBW2021 / Agenda Created Live Each Day

Day 1 Monday March 8, 2021

SESSION 1

1A/Phones – Friends or Foes! / Didn't happen?
1C/How to Distinguish Between Products with Goo Biomentric Stewardship from those Without
1D/ Deviceless solution design using biometrics for financial interactions (au naturel vs implants, privacy, ethics)
1F/Social Impact of Biometrics

SESSION 2

2A/Ethical Use of Biometrics
2D/Voice Biometrics – As a Factor in Identity Access
2C/Biometric Software Development

SESSION 3

3A/Conversational Voice AI – B2B and B2C Standards
3C/What is Self-Sovereign Identity
3E/Deepfakes & Biometric 101

Day 2 Wednesday March 10, 2021

SESSION 4

4A/ Using Biometrics to Unlock a Cryptographic Keystore
4C/ FIDO-what is it and certification

SESSION 5
5A/ Biometrics and SSI - How / Where Does It Fit
5E/ Biometric Deepfake Use Cases/PoCs 201

SESSION 6
6A/ Biometrics for Different Ages: Examples, Issues, and Future
6B/ Biometrics and the Role of Open Source

Day 3 Wednesday March 12, 2021

SESSION 7
7A/ The Privacy, Accessibility, Inclusion and Diversity (PAID) framework for Biometric Technologies
7E/ Biometric Incident Response

SESSION 8
8A/ How does SSI, FIDO, Physical and non-physical Biometrics, Identity and Authentication all fit together, for privacy, security and Compliance?

SESSION 9
9A/ Optional: DID (what is it) and how did Biometrics come (and go) in w3c/did-core
9D/ COVID-19 Focus: How has the pandemic impacted biometrics? And what are ethical concerns related to health data collection?

Monday March 8 / Sessions 1 - 3

Phones - Friends or Foe!

Session 1A
Convener: Eric Welton
Notes-taker(s): Wade & Eric

Please list the key points of your conversation and/or what you would like to share with your colleagues.

With Apple/Android using biometrics for security, and increased AI-driven awareness of the individual - they need to have a clean line of perception, without the possibility to introduce deepfakes and other identity protection. However, when using these devices to communicate "upstream", we are presumably allowed to protect our identities and digital dignity through the use of biometric filters that render us unmatchable or privacy protected (in the case of behavioural biometrics, like voice/video).

There is a layer of absolute and unmitigated trust between users and "some place in their device", and then a general distrust of the internet. Is the absolute and unmitigated trust in Apple corporation, Android phone makers, Google, and others warranted - or is the reality simply too terrifying to face directly, resulting in a belief that "they must be safe, otherwise They would not be allowed"

Maybe it's about the biometric direction of travel and ownership/inheritance

Parts Social Impact (Social Impact of Biometrics, Kim Green) and place of residence for biometric federation

Layer 1: Deepfake layer
Layer 2: Encryption
Layer 3: Video Transmission
Layer 4: OS/Drivers

Which biometric modalities did your group discuss? Check all that apply

[x] Face [x] Fingerprint [ ] Palm [x] Iris/Eye [X] Voice [ ] DNA
[x] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**
[x] **Accessibility Risks**
[x] **Inclusion Risks**
[N/A in this context] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?

If YES please provide Contact Information for those who are interested:

Continuation of research, and how to meet the best of all compliances,SECURITY and Privacy!

Anyone who has questions I can answer or answers they find to questions I asked, can contact me via LinkedIn Brian Clinkenbeard | LinkedIn , or my private email brian@interjacence.com

https://us-cert.cisa.gov/forms/csetiso CSET TOOL referred to that offers cross compliance mapping as part of assessments for NIST with BIOMETRICS, Auth and IDENTITY specific requirements….
Thanks for a great conference!

Brian Clinkenbeard
CIO/Director of Security
NimbusID
A Non-physical cognitive biometric for auth and intent implied Identity

How to Distinguish between Products with Good Biometric Stewardship from Those Without.

Session 1C
Convener: Dena B. Mendelsohn
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

- **How do we trust the organizations that manage our personal data?**
- There seems not to be a standard way to track transparency and forthrightness of orgs
- **What is the link between privacy policy and software development?**
- Progressive identity - only collecting data as it is absolutely necessary ("progressive disclosure")
- What are best practices around securing and tracking usage intentions of data?
- Medical data was once stored in a manilla folder in a file cabinet with lock and key and managed by keyholders. Now, with the internet, all of that data is stored online. That data is no longer living with the subjects of the data.
- Question is around security of hardware and software and ethics of developers of these systems
- Leaks happen from third party orgs
- There should be HIPAA regulations around why data consumers are consuming our medical records but there are not and that is a major gap.
- Do we need a UL for data safety? Yes probably. But who would that be?
    - FIDO (fast identity online) has a certification program for biometrics used on the phone. Has different levels that lay out security requirements, which are publicly available. They use

    - certified labs that check whether companies are meeting the requirements as they are laid out.
    - With FIDO, there is a process for collecting, protecting, and verifying data
    - iBeta is a vendor that does review work
- Primary security issue is data that is hacked out of the system. NIST, SOC, etc. are adequate for individual devices and the real issue is how all the data in the system is secured
- How do we keep track of the full spectrum of consumer devices that can capture or expose sensitive data (e.g., Firby banned from U.S. gov't property due to infrared memorization)
- **Data rights and security practices must be treated separately**
- If a company does not have a privacy policy that is a major red flag
- Elektra Labs consumes privacy policy from companies and emits understandable data
- MDS2 form may supply useful info for security practices but not frequently posted online by companies
- Infoguard is an important organization that discovers and discloses security vulnerabilities before it reaches the public
- Compliance should be broken down to the separate components (software, hardware, etc.)

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**

[ ] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Deviceless solution design using biometrics for financial interactions (au naturel vs implants, privacy, ethics)

Session 1D
Convener: John Miedema
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

This was an open discussion to get opinions on different topics related to digital cash and the use of deviceless solutions and biometrics:

- Central Bank Digital Currency research phase, cash-dependent people, user interaction with money, smart phones biometrics, custom devices, deviceless biometrics solutions, possible implant
- Other topics: all the compute on the merchant side, who owns the records of my interaction, accessibilities, downsizes and risks, facial profiling, racial profiling

Key points during discussion:
- ethical considerations,
- biometrics reveal medical data,
- privacy considerations,
- different cultural issues related to privacy,
- digitization of banking system and its implications,
- biometrics as authentication use data stored by a 3rd party vs self-sovereign identity
- digital driver license,
- decline in the use of cash- examples in Europe-only digital,
- unbanked people,
- ZKP and threshold cryptography, homomorphic encryption, secure multi-party computation can still provide privacy and security
- identity proofing against network, the need to be connected vs all the computation related to biometrics are local,
- biometric proofing without connection to the network,
- liveness detection

Which biometric modalities did your group discuss? Check all that apply

[X] Face [ ] Fingerprint [X] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[ ] **Accessibility Risks**

[X] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
No
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Social Impact of Biometrics

Session 1F
Convener: Kim Green
Notes-taker(s): Thank you to the notetaker (?)

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Social Impact of Biometrics
Get more technical understanding
Why are we doing this to begin with.
I'm not sure it seems obvious - we start in a direction and then follow suit.
What some of the social impact is.

As Scientists, human beings,
Turning around once start down path.
How is it currently used, how it is accepted, how

Technically and ethically.
Where the convener is coming from - been in tech for 30+ years. Sit on a lot of boards. Secure lifecycle development. If you knew how they developed their products you would be concerned.
Genetic Data - they are not being good stewards of our data.
So you will be lucky if Biometrics is being used.
Two factor - Multi Factor - security control to identify who is there to access a system.
- SMS
- Authenticator tool such as google.
- Know

How you do it - Behavioral
Where you do it - Geolocation
I still use pins - Not trusting of Biometrics yet
We always assume that it is just going to be us.
Served in military - it isn't always a nice place.
In war using facial biometric - there is nothing to stop someone from forcing you to use it.

Privacy Rights
Concern about rolling them out.
Concern about biometrics being used by law enforcement.

You are pulled over - you have a phone - they can force you to use the finger to force someone to open their phones.

One aspect relating to the social impact - tomorrow we all die. What happens to our biometric essence - pass it along to our children.

Technology giving us the means to use biometrics for a whole spectrum of things.
What happens to my biometric identity who gets it an who gets to maintain it.

I'm a big user of 3D printing - 3D Tissue printing - genetic reprinting.
Genetic data available in 23&Me

In Security - this bothers me.
Maybe one data breach multiple data breaches and can compile together - launder for legal commercial use.
Taking all this information together.

Many people getting together from different industries - when all these industries come together they create issues.
Social Element
Familiar with UN SDGs
Concept of one of the goals is to provide everyone in the world with an identity they can use. (16.9)
It is an honorable goal - we may be able to do it.
People can't get access to commerce and other things because they can't figure out who I am.
Institutions are requiring ID to do transactions.
Refugees - my country is at war and left in a hurry - didn't take pieces of identity - how do I get access to resource. Biometrics - way to prove who I am - to access food, shelter.

16.9 about getting all inhabitants getting legal identity (For inclusion) + birth registration.
UNHCR - BIMS - biometric identity management system.
Do talk about how to uniquely identify refugees
And then the questions can that UN- ID used outside of camps. ID2020 comes into create systems that fulfill SDG 16.9.

What about Refugees getting to choose or not.
Not financially stable people in refugees - how do they get to choose.
World War 2 in Germany the reason they were successful in rounding up jewish people because of good record keeping systems.
Important to remember not all used for good
Identity connection to land ownership - and owe taxes.
"The Them factor"
Them could be any number of entities individuals.
Focused on the human operating system.
All of this code work on human operating system - the way that our bodies/minds/brains work
Our biometrics are our "firmware" I'm concerned about how to immutably hold on to them.
Are they

Comment - biometrics and migration - this is her focus.

Issue of tracking biometrics for migrants.
Fixes them in time and space.
European Fingerprint DB - when they first enter the EU fixes them in the first country they arrive in.
Country is in Italy even if they have family in another state in the EU.
It is exposing very vulnerable people with very limited.
Their Biometrics get stored in large biometric databases.
Concerns about how these systems are being used on migrants and refugees.

The system is called EuroDack

One for law enforcement
One for migration
One for _____

They were asking member states to biometrically enroll children - for positive social impact - trying to stop child trafficking.

A lot of what is going on is need to create policy to address issues.
Always have to look at the negatives.

Person speaking helped on Aadhaar - worked on that systems. How to get 1.3 Billions indians support they deserve. Each individual is enrolled to get aadhaar number - so each individuals.
Was supposed to be opt in - a lot of negatives that were ironed out via policy. The idea was to be inclusion for positive social impact - but it exposed negative social impact.

Follow-up comment - what was mentioned about firmware.
Wondered about passage of time - mutable or immutable.
Fingerprints change - burn with acid.
To what extent the concept of the ship of Theseus applies.
No specific formulation - if you go through innovation of cells - 2-3 years you have totally different cells.
Mitosis. Telimers.

Based on a very small variability.
Component of time passing.
Percentage of error intake.
Time does seem to have a component.

The integrity of biometric data over time -it becomes obsolete.
Capturing digitally biometrics - has validity - comparability - to templates.
Depends on lots of things

The THEM factor - herding and nudging and that is the socially - psychically.
They oriented people against the community - via propaganda - what excites them at a rally.
At a nation state level - countries are worried about deep fakes into catalyzing their citizenry to do crazy things. (as we are seeing).

15-16 and beyond these biometrics are fairly stable.
  Fingerprint, face, iris.

One reason that our passport - ICAO compliant - the one that is required is Face. Suggested not mandatory that every 10 years you get a new one because of facial aging.
Biometrics are fairly stable from 16-60.
Infant biometrics is being done.
Fingerprints are stable 5 years and above - but re-enrollment time is more frequent - every year or three years.

The question - governance and policies - will they be adequate?
Compliance is not security.
My worry is: Will these things actually be secure?

Reason brought this up GDPR - good attempt not perfect but good attempt. Forget the word biometric for a moment. We have documents out in the world that identify us - biometrics is a new attribute of ours. So it is more the governance of biometrics as an attribute. Focused on data collection. Permission levels.

Key with biometrics as well.
Biometrics just as valuable as

Works with organizations that do work with voice biometrics.

Business rules.
Biometrics - should consider having analytics to determine overall position at time of doing it.

Does biometrics software do this now?
I don't use facial recognition - doesn't work before coffee - it doesn't know that it is me…

People were having bad things happen.
Enroll - ring figure as finger of DURESS.
Need a savvy client.
Need things to be there that
Need to understand the tech - to delay evil.

On the other side of the coin using these things under duress.
Give away - trying to regain ID in critical moments. Trying to regain access.
Duress of people giving the data.

Like to talk about the security of biometrics themselves. How is it deployed?
NOt sure if asking the right question.
Come back to concerns about policies and security aspects - GDPR is a good start.

Scenario.
Have regulation - not overly prescriptive.
Right to be forgotten.
That requirement - it is almost impossible. As far as most organizations concerned.
IN order to do that - might affect integrity of another system -
Delete primary databases - and unstructured data.
Rarely remove from backup systems -everyone knows about it.
How good are these laws if they are only somewhat going to implement comply.

How is biometric software developed?
Is it done in a secure manner?
Looking at it from everyday implementation.
Issues around complying - talking about a lot of technology debt.
The people who are doing this are not very well skilled.
In security alone - we don't have security analysts - administrators of security tools. WE have securitied us.
This is what has concerned me.

We need to do a threat model.
They don't even know how to do a threat model or what a threat model is..
Losing the ability to do that and security vendors are

Share something about the last discussion - about likeliness of facial recognition - do research on behavioral biometrics - knowing how you type and how to identify you. When you are under duress you type differently. The way you are typing this is "not you" it seems that you are typing in a different way.
We can detect duress from that.
From facial recognition - there are studies about how to determine the mood of a person from facial recognition.
I'm not sure that the fingerprint system can detect - can detect liveliness but not duress.
Point: want to test sweatiness.

I believe the best form to be more secure with biometrics data - people should hold their own data. There are a few concerns about that - biometrics data needs to be held by the government for human security to know who is dangerous.
Some of the users that interview - prefer convenience over security.
If we say that we want you to own your data.
What if I used my computer - my data on my phone.
Concern - prefer people owning biometric data would have been the best.
People prefer convenience over security.

So many things said - that were ah-ha.
Everyone should own their data.
Shared responsibility model. (our data but we are allowing them to have it) are they good stewards of our data.

Having served 8 years in the military. Security is an illusion. It is - we can put in a lot of controls. There is no control that can keep someone completely out of that system.
When more and more people willing to give up convenience

Military does everything to break you down and build you back up.
Give up liberties for amenities - until, one day, those liberties are no longer there.

What about culture and responsibility?
Biometric definition in chat.

You have to be brave to jump right in to anchor on of the first sessions! Thanks Kim!

I'm in the notes for Session 1F if you want to help me take notes.

Why do I have the impression that we are looking a biometrics (in the context of this conversation) as a key? It opens doors so the same problematiques key have (custody, maintenance, delegation, you name it) apply.

The only difference I can imagine is that a traditional key is "external" to me, there isn't a necessary connection between it and myself while biometrics obviously do.

EU also wants to combine all three of those in one massive database called CIR as well
(common identity repository)

Giving access to our bio-metrics is granting code to our human firmware running our HumanOS. At the point, herding and nudging becomes all the more possible. Grants conduits to our HumanOS.

Will governance policies be adequate? access by multiple factors, audits, ?

GDPR is a good attempt at policy around data protection / privacy / transparancy

focus on data handling lifecycle (inclusive of biometrics?)

"Eye" wonder how long an iris stays "the same"?

Lifecycle >> Sampling frequency , which makes me think about lossless vs loss-some(?)
New photo = sampling frequency

Thanks! Nice to know the validity...

Social Implications?

GDPR has two general categories : personal data and SENSITIVE personal data - biometrics (and health) fall into the latter

More than one factor is what we use IRL.
Voice and face don't match == Uh oh.

Creepy Fact: An eye has been used to pass through a biometric door sensor effectively up to 27 hours after it has been out of the head...

Were'n't there some solutions implemented to detect "alive/connected" bio IDs such as fingers having a pulse? I remember seeing that decades ago.
I can imagine eyes amy also have such parameters available?
Ya rev 2.x seeking blood cell pulsing deep in there! ;)

Video analytics can be used for emotion detection - this is NOT BIOMETRICS (according to the ISO definition)

That is then a connundrum as we can then not talk of "detect duress through biometrics".
Unless other parameters are used aside from face?
(do neurochemicals follow patterns that we can consider biometric?)

I think we are almost out of time... right?

People perceive a minimal sense of "cost" to giving the data for convenience. What is the COST of the convenience. The greater the convenience, the less the cost seems to matter at decision point moment. The greater the perceived value of the convenience the more the cost seems to be mitigated by the ether of the convenience.

I'm simply saying that emotions are not physiological or behavioral characteristics that can be used for uniquely identification

Which biometric modalities did your group discuss? Check all that apply

[X] Face [X] Fingerprint [X] Palm [X] Iris/Eye [X] Voice [X] DNA
[X] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[ ] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Ethical Use of Biometrics

Session 2A
Convener: Dan Bachenheimer
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

General theme for many participants is that Regulation is critical to defining and identifying the ethical/non-ethical use of biometrics - and that Regulation is heavily waning.

Two Categories: (personal privacy) where the user fears about the safety of his unique biometric identifiers vs (informational privacy), where the user fears about the misuse of his biometric information and "function creep". (Source)

Principles (Source) regarding biometrics data collection and usage are listed below:

- It should be collected fairly and lawfully
- It should be used only for the purpose specified during collection
- It should be accurate, up-to-date and stored securely
- It should be accessible so that individuals can verify and correct their data
- It should be disposed of once the specified purpose has been achieved

Consent around Biometrics in a situation where there is a power differentiations.

Consent

Sharing photos in Facebook - what about them being uploaded before they could be recognized.

How about

On board of biometrics institute - we have ethical principles.
Informed consent -
Do for good not evil.
It is evolving - try to refresh as area matures.

Ethics connected to trust?
If we consent to sharing out personal information
In GDPR - data controler and data processor.
If I opt to share personal data - so data processor can processes it on behalf of a data control- they must tell me why, who they are going to share it with, how long they will retain it.
If i have right to be forgotten.
I have to trust that the data processors under data controler control will delite.

We have a right for data portability - give me all the informatoin they have on my - must trust that they will actually will provide it.

To what extent about various agencies can get away with whatever they want.
Is “ethics” an opt in.
“Gun control” is a opt in in that it doesn’t affect

Possession of 1:N search capabilities should be made illegal.

Examples of non-ethical use didn’t opt in, no informed consent.
NO real oversight or regulation that will protect us.

I remember 9/11 was on an FBI contrat.
Where these laws came up where we give up certain freedoms.

Chief engineer - global entry - to DHS not supposed to have fingerprints - i Opted in for expedited clearance.

Lots of over - reach on the surveillance side.
They trusted the government for their benefit like global entry - rather then private sector.
When they are overt - privacy impact assessment - system of record

Can’t speak to covert use - lots of things done that i don’t

On the Overt side there are certain benefits.
Terroists watch list.
We would get fingerprints - IEDs - we would be able to identify them - they didn’t opt in but could be considered a

One person’s terrorist is someone else’s freedom fighter.
In the past we were using similar arguments against homosexuals.

False positives can lead to harassment

Banning Facial recognition - a reason for doing that is about accuracy and racial bias.
1:1 authentication in controlled - opt in environment.

If it is a surveillance camera outside with no lighting control and at a distance - the way the physics works it will have a higher error rate - candidates list going up.

Supportive in theory - in not having terrorists
Used as an excuse to collect a lot of data
Iraqi and Afghan database - ABIS DB - enrolling every
Fingerprints from Sadahm era criminal records.
Idea of terrorism gives these institutions a lot of
Allowed to store these IDs indefinitely.
Even if we have these justifications that seem to be legitimate they need to have guard rails
Can people request to see records.
ABIS - Automated Biometric identification System (fingerprint, iris, face).

digital anthropologist.
There is a layer where survival of larger group - we need structure, trust ethics for a larger society.

Different groups
We are human animals - in contested space of resources and power wants.
People present themselves in society -
Need to address - with people acting out.

trust and ethics need work and thats what the entities or corporations need to do

Ethics around
The location of where the data is stored - important in ethical
Maybe blockchain can help?

Biometrics and Forensics Ethics Group (BFEG) released an ethical framework to guide the technology. (Source)
> policy sponsor (Alex Macdonald) asked the group to consider police use of facial recognition systems and subsequent report identifies nine key ethical areas that should be considered when designing policy and deploying technology
> participants: Professor Nina Hallowell, Professor Louise Amoore, Professor Simon Caney and Dr Peter Waggett

“Developers have sought to diversify their data sets, even if it means generating images through simulation.” (Source)

Proper securing of image databases, such as local storage

Governments at all levels are creating task forces to analyze responsible ways to use facial recognition for public safety without compromising ethics (Source)

Comment from Chat: the problem is the changing face of what it means to "want to be a part of the society" - you mean, "adheres to conservative white christian values?" - or did you mean "a progressive attitude of tolerance and openness" - the reason I have changed my opinion of organizations like DHS from "valuable" to "my mortal enemy" is because of the increasing white power nationalism of the united states and the reduction of basic livability within that society in the name of technical gadget addiction and hyperbolic consumption.

Comment from Chat: Society in terms of fitting into a place that serves you well and vice versa. The ever challenging and changing landscape of cultre/power politics (local aa much as global) can change the face of a friend into a foe based on influencers and intentions thereof...

Comment from Chat: Should have only been used that way with probable cause signed off by a judge...

Comment from Chat: i wonder if the question is not the ethics of biometrics, but the degree to which biometrics can amplify bad behaviour in a non-ethical society - e.g. if the society itself is incapable of behaving with civility and decency, then biometrics will amplify those bad habits.

If it is surveillance and you patch against a watch list - it is a lead generator.
Practical matter that law enforcement makes in real life - the detective - sends photo IDed by the system. It taints the person’s memory

Comment from Chat: Unethical?!: Using past information, the giving of which was at one time not a culturally threating/distasteful, against someone is a woeful practice these days.

Comment from Chat: so are understanding of the organization change according to ideology...?

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[ ] **Privacy Risks**

[ ] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Biometric Software Development

Session 2C
Convener: Kim Green
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Software developers can be confused by biometric SDKs that yield probabilistic results (instead of yes/no) booleans. When combined with liveness counter-measures, the development task can be comlex, ripe for misconfiguration or incorrect business logic. We discussed how (or if) risk can be understood relative to biometric identity, authentication and authorization systems. AI seems inextricably linked to biometric systems in this regarding. This brings up all the AI bias issues with biometrics.

Which biometric modalities did your group discuss? Check all that apply

[X] Face [X] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[X] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[ ] **Accessibility Risks**

[X] **Inclusion Risks**

[X] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Voice Biometrics - as a Factor in Identity Access

Session @D
Convener: Michael Novak
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Discussed voice pros & cons as valid component of MFA for IAM

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [X] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) ___ _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[X] **Accessibility Risks**

[X] **Inclusion Risks**

[X] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Conversational Voice AI - B2B and B2C Standards

Session 3A
Convener: Michael Novak
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Voice is a viable biometric and used extensively in many applications. It has spoofing issues (generative adversarial networks for example) but can be convenient when combined with other modalities and security measures. Picovoice, #VoiceLunch (on Twitter) and Open Voice Network project also mentioned.

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [X] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[X] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

What is Self-Sovereign Identity

Session 3C
Convener: Kaliya Young
Notes-taker(s): Chris

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Kaliya Shared Slides There was a good discussion.
Here is a lnk to not the same slides but a deck that explains SSI.

Protocol layers: Where is the protocol for Level 8?

OpenID: ID for one service is used across several

Opti

- Everyone has their own id

- phone number

- _____

The problem is that these are all "rented"

DID = decentralized Identifier

How to define keys so you're not locked into one public place

Standard elements of a DID doc:

Governments are very excited about using biometrics for identification

A verifiable credential has to do with the cryptography alone; it doesn't reflect whether the data is true or not. That truth must be verified outside of the system.

The verifier does not speak to the issuer.

No PII ends up on the shared ledgers.

There's an effort to end the use of usernames and passwords

Infinitely scalable low cost federation

ktdi.org

very concerned about the MBL standards because they're closed.
There are several Canadian provinces looking at implementation of these types of standards.

types of data storage:
centralized, federated, decentralized

The matching happens on your device, not the verifier's; so, your wallet doesn't open

DID documents are not intended for people; they're for verifiers and issuers.

Chat notes:
Cyrus Minwalla to Everyone (12:36 PM)
Curious to hear the views across the table.

I suggest checking out: ktdi.org

Verifiable Credentials Flavors Explained
https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/

Biometrics
https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/draft-documents/Biometrics.md

Matching hashes is deterministic whereas biometric matching is fundamentally probablistic
Excellent point

I have a lot of questions around how this would intersect with migration. Looks like there are some early academic studies about that, so I'm looking forward to digging in to learn more.

I think FIDO is probably the answer

It's the end of the session…so lets head back to the main room.

where biometric matching is done locally on user agent which can be verified cryptographically by the relying party, and then generates the ZKP on user agent for proving my identity to relying party

Which biometric modalities did your group discuss? Check all that apply

[x] Face [x] Fingerprint [ ] Palm [ ] Iris/Eye [x] Voice [ ] DNA
[ ] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**

[ ] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are int

Deepfakes and Biometric 101

Session 3E
Convener: Wade Bittle
Notes-taker(s): Wade
Participants: KimG, JeffO, JeffK, Tod Gehrke

Please list the key points of your conversation and/or what you would like to share with your colleagues.

This subject was new to the participants (editors comment).
As such I've added a Resource section at the end.

Deepfakes (synthetic media) spoof a live presence of a real human
> "all senses of person is lit up" (JeffO)
Deepfakes are malinformation a derivative of misinformation (def., Pew Research, see all difference here)**

> Fooling - experience/engagement moves fast
> creates sockpuppets, non-existent persons, active both online and in traditional media
> Deepfakes vs Shallowfakes (read here, see Jim Acosta interview for shallowfake example)
> Deeptrace cybersecurity researchers found 14,698 deepfake videos online, compared with 7,964 in December 2018.

Acceleration/Amount of Data:
Being at the top of the data acceleration curve: in addition to internet system access, to a banking system, to an electrical grid and infrastructure, the ability to produce a very realistic fake video completes the adversarial foundation

Seeing is Believing, though more to truth, Believing is Seeing: Human beings seek out information that supports what they want to believe and ignore the rest. (Source)

Hacking that human tendency gives malicious actors a lot of power. We see this already with disinformation (so-called "fake news") that creates deliberate falsehoods that then spread under the guise of truth. (Source)

A. Deepfakes exploit generative adversarial networks (GANs)
> two machine learning (ML) models duke it out
B. ML Training Model 1 trains on a data set to create video forgeries
A. ML Training Model 2 attempts to detect the forgeries.
A. Forger creates fakes until the other ML model can't detect the forgery.
Notes: The larger the set of training data, the easier it is for the forger to create a believable deepfake. (Source)

comparison (?): magic tricks that fool the mind through illusion or NPCs (non-player character) in sims (Example 1, 2, 3, 4) and their associated behaviour or dialogue (warning: the videos are trippy)

cybercriminals started using photos and pre-recorded videos to bypass biometric-based verification systems a few years ago (here and here)

underlying technologies and use cases for facial recognition (non-consented) and facial authentication (consented) are different

Participants Input

Proprietary and Trust could become central
> confidence, integrity and discrediting are real sub-concepts here
> trust registers maybe (?)

Should we modify the blackbox mentality…?
> products that are not explainable
> parochialism rears its head bolstering the silos

Shortcuts are taken in the softDev lifecycle (from a CISO perspective)
> "Core of What You Do Matters"
other participants
> certifying open source properly…?
> quit economizing ("found out shortcuts dont get us to target A")

Facial recognition would be most impactful in creating mayhem

Liveliness* could prevent deepfakes through individual patterns

* Types of Legacy *liveliness detection*: blink, smile, turn, nod, watch colored flashing lights
> can easily be spoofed by deepfakes and advanced spoofing techniques.
> currently the only lab performing presentation attack detection (PAD) testing guided by the all-important ISO 30107 global standard
> noteworthy since Level-2 test attempts to spoof tech using live human test subjects wearing realistic 3D masks
Note: Certified liveness detection is performed by iBeta, a NIST/NVLAP-accredited lab and attests to a solution's ability to defend against advanced spoofing attacks

(Source 1, 2)

from Chat:
**The phrase "mal-information" was also brought up @ IIW in the Deep Fake Info type I
https://womeninidentity.org/2019/11/05/kathryn-harrison-deepfakes-deep-trust-alliance/ (JeffO)

RESOURCES

https://www.biometricupdate.com/201912/digital-identity-predictions-for-2020-biometrics-deepfakes-cybersecurity-and-decentralized-id

https://techhq.com/2020/08/deepfakes-ranked-by-experts-as-most-serious-ai-crime-threat/

from Chat:
https://www.linkedin.com/pulse/deepfakes-disinfo-101-reading-list-kathryn-harrison?trk=public_profile_article_view (JeffO)

Deep Fake Tools (1, 2)

Deepfake Report Act of 2019 (S. 2065) passed the Senate on October 24, 2019

BOT Disclosure Law (California)
> making it illegal *"for any person to use a bot to communicate or interact with another person...with the intent to mislead the other person with its artificial identity."*
Rep. Yvette Clark (D-NY) June 2019 introduced the *DEEPFAKES Accountability Act*
> when passed, would require the creators of false videos to label them as such or face up to five years in prison.

Standard deepfake detection models analyze videos frame-by-frame to spot any sign of manipulation.

New tool developed by USC Information Sciences Institute (USC ISI) researches
> focuses on subtle face and head movements & artifacts in to determine a fake video
> identify the computer-generated videos with up to 96%
> requires far less computing power and time, reviewing an entire video all at once
(Source)

Microsoft Video Authenticator
> analyze a still photo or video and provide a percentage chance that the media is artificially manipulated.
> developed alongside Microsoft's responsible AI team and AI ethics advisory board
> works by detecting the blending boundary of the deepfake and subtle fading or greyscale elements undetectable by eye alone
(Source)

Detection tools may not be enough.

DeepTrust Organization (6 layers); government (17 layers)
(JeffO)

Which biometric modalities did your group discuss? Check all that apply

[X] Face [X] Fingerprint [ ] Palm [X] Iris/Eye [X] Voice [ ] DNA
[X] Behavioral [ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] Privacy Risks

[ ] Accessibility Risks

[X] Inclusion Risks

[X] Diversity Risks

Note: Liveliness Tests should be culturally appropriate

[discussion from March 10 imported here]

Cultural Issues: Labeling of Data
> which databases of demographic data (look further)
> large datasets to offset bias
> crowdsource for face

Workplace: discriminating impacts/biometric screening
> differential biased operation (http://gendershades.org/ [from chat])
> performance deviates in different cultural groups - want to normalize the error rates (StephS)

from Chat: (cutural biases)
https://www.npr.org/2020/06/22/881845711/tech-companies-are-limiting-police-use-of-facial-recognition-heres-why
https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?

Take Survey: https://survs.com/survey/owy945xu2u [Updated]

Call-to-Action:

To implement futures measures there needs to be *strategy* and *stewardship*, as well as *consistency* and *foundation* for *interoperability*.

One manifestation/implementation could be an everyday deepfake biometric tool.
Merging basic deepfake detection with trust/identification chain (a start)

Comment in Chat: "There being too much constantly changing data and ideas and techniques makes it very hard to build any *useful infrastructure and useful abstractions that can actually allow us to progress in a*

*helpful direction***.** That means we have to rely on a few experts to support all of us and all of our needs, which isn't scalable and is too easy to take advantage of. You can't build a standard if the foundation is shifting underneath you"

If so, can other's from the workshop join?

Yes the sub-committee around sub-sovereign identities

If YES please provide Contact Information for those who are interested:
(due to privacy I had left it to organizers to pull contact)
KimG
JeffO
Todd Gerghty
WadeB

Tuesday March 10 / Sessions 4 - 6

Using Biometrics to Unlock a Cryptographic Keystore

Session 4A
Convener: Eric Welton
Notes-taker(s): Eric Welton

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Setup of the question

Deterministic operation so there wouldn't be a need for the intermediary step?
Biometrics key generation

- Either imposter (helper data) or time-intensive
- There is some work done on biometric cryptosystems where biometric can be used to generate key or bind key but these approaches always have the issue of degrading performance. Also, you have to setup helper-data with this systems which can be a security hole in some techniques

Homomorphic encryption
Hashing biometrics

- 1-way functions with probabilistic considerations

Where is the use-case coming from.
Unlocking the confidential data store.
Template stored on device/in cloud.

Which biometric modalities did your group discuss? Check all that apply

[x] Face [x] Fingerprint [ ] Palm [ ] Iris/Eye [x] Voice [x] DNA
[x] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**

[x] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

FIDO-What Is It and Certification

Session 4C
Convener: Stephanie Schuckers
Notes-taker(s): Dena Mendelsohn

Please list the key points of your conversation and/or what you would like to share with your colleagues.

https://fidoalliance.org/

Replacing passwords, SMS, other knowledge questions to something better; there is still room for even better. Right now, you can choose the FIDO authenticator that you trust more. The consumer can be selective but the company has to choose an option that will be accessible to as many people as possible
Authentication – you prove yourself to your device, your device proves itself to another party
The way you prove yourself could be biometrics, a pin, etc.
Device proves itself via public key cryptography
Public/private key – private key stored in device, public key goes to the other party

Later, prove yourself to the device, private key is unlocked, key sent to relying party that confirms the public key is valid

Is the certification procedure documented

https://fidoalliance.org/?s=certification&id=28805

Data (keys plus biometrics data) and algorithms are certified as different levels of security authenticators can be run on mobile and laptops

The relying party runs a FIDO server to communicate with FIDO devices

https://github.com/cedarcode/webauthn-rails-demo-app

https://fidoalliance.org/certification/biometric-component-certification/fido-accredited-biometric-laboratories

https://fidoalliance.org/certification/authenticator-certification-levels/accredited-security-laboratories

You can authenticate yourself on multiple devices with FIDO via a process to "register" them.

The biometric data is stored in the physical device (authenticator)

Example of mis-registering a person: a bank that is linking the biometrics of an individual to an account needs to make sure that is actually the biometrics of the intended individual.

Why aren't there digital notaries already?

Identity Verification and Binding initiative — creating a set of ways for binding authentication

Read John's article:
https://medium.com/thoughtful-biometrics/being-thoughtful-about-biometrics-1f28ac2a27d5

Question: is using biometrics the best answer to address the issues with password authentication?

IDs, such as a driver's licenses, can be faked. If you can reduce the proximity to the device and know it's you holding the device, that's a much lower failure rate by many magnitudes.

FIDO has a white paper on account recovery (FYI here's FIDO white papers)

COVID has accelerated the rate that people are asked to operate remotely; this has created inclusion impacts, such as for individuals who live in remote areas. Having to physically attest for identification verification creates access issues. FIDO Is working on the problems with binding, it's a work in progress.

FIDO has two parts (1) user to device through biometrics (or pin) plus (2) device to server

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[ ] **Privacy Risks**

[ ] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Biometrics and SSI - How / Where Does It Fit

Session 5A
Convener: Todd Gehrke
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Starting off with discussion of where biometrics fit into the SSI flow.
In the DID spsication calls out verification as well as authentication

Verification Methods

1. *5.2.1 Verification Material*
2. *5.2.2 Referring to Verification Methods*

5.3 Verification Relationships

1. *5.3.1 Authentication*
    1. *5.3.2 Assertion*

. . .

This is useful to any authentication verifier that needs to check to see if an entity that is attempting to authenticate is, in fact, presenting a valid proof of authentication. When a verifier receives some data (in some protocol-specific format) that contains a proof that was made for the purpose of "authentication", and that says that an entity is identified by the DID, then that verifier checks to ensure that the proof can be verified using a verification method (e.g., public key) listed under authentication in the DID Document.

. . . .

The question is should biometrics be included in the authentication flow of the connection protocol OR should it be handled as an assertion as part of a verifiable credential.
Dan B -

- Provided overview of work he had done with the trusted traveler where the biometric was part of a VC.
- Highlighted the need to store the raw biometric image and not just the template.

Jack -

- Reference to NIST standard on physics of contactless capture [Nist 8307]]
- Three types of biometrics: raw (picture); processed (black and white image); minutia- vectors represented as string of x,y,z coordinates - algorithms used to recognize underlying relationships in a set of data through a process that mimics visual inspection

- Open question is how best to perform biometric authentication within a VC model:
    - Should the authentication method be linked to a biometric service from the DID doc?
    - Should the authentication method be a stored as part of the VC itself;
    - Future state: a biometric service performs the match, then the underlying data gets deleted. Future future state: a secure virtual machine is created, performs a match, then deletes itself. - The would be done in a secure enclave.

- **Centralized storage of biometric data is unsustainable**. Though orgs like Clear and governments hold (or contract processing of) large amounts of biometric data today, there will likely be a move towards decentralized storage over the next 10 years;.

Which biometric modalities did your group discuss? Check all that apply

[X] Face [X] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[X] **Accessibility Risks**

[ ] **Inclusion Risks**

[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Follow meeting on day 3 -

Deepfake Proofs and Biometric

Session 5E
Convener: Wade Bittle
Notes-taker(s): Wade Bittle, Supreet & Stephanie
Participants: Sunpreet Arora, Stephanie Schukers, Katrina Ingram, Daqing, John Mediema, Emmanuel Marasco

Take Survey for Day 3: https://survs.com/survey/owy945xu2u [Updated]

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Shifted from "common use cases" to concerning the "whole biometric chain" and at what points in the chain could certain attacks happen.
Some good but minimal discussion on attack types.

Why use biometrics…? (is it settled on biometrics) (Katrina)
Is there alternative to biometrics that is as convenient but less impact to privacy..?

Part of Answer (?): Secrecy (liveliness device) doesn't mean its useful (Stephanie)

Liveliness* is based on trust from the client

Is there a discussion about transfer of liability or risk…?

ML Model in background verifying liveliness (Sunpreet)

Where in the biometric chain are the attacks…?
> Deepfake Attacks on Biometric Liveliness
> persistent rootkits the hardware level
> PAD attacks

Digital Injection with masks (Sunpreet)
> projecting patterns in physical space (https://arxiv.org/abs/2003.11145 [from chat])
> Client-Side Cameras, Remote (projector)
> untargeted attack

External Illumination Attacks (mobile projectors)

1. Hardware Module/Capture Device (Client-Side)
2. Liveliness (Second external device)
3. External Source (photonic, laser/ultrasonic)

* Types of Legacy *liveliness detection*: blink, smile, turn, nod, watch colored flashing lights
> can easily be spoofed by deepfakes and advanced spoofing techniques.
> currently the only lab performing presentation attack detection (PAD) testing guided by the all-important ISO 30107 global standard

> noteworthy since Level-2 test attempts to spoof tech using live human test subjects wearing realistic 3D masks
Note: Certified liveness detection is performed by iBeta, a NIST/NVLAP-accredited lab and attests to a solution's ability to defend against advanced spoofing attacks

(Source 1, 2)

Biometric hacking becoming commonplace
> tackling coerced biometric authentication

PoC 2020

4 Major Attacks: 2D and 3D masks, replay attacks and coercion
> National ID cards found to be the most frequently defrauded documents, the report adds, citing the Indonesian, Italian and Polish ID cards as the most frequently attacked

(Source, Onfido Report)

PoC 2008
Concept: "Biologging" (Matthew Lewis, British security researcher) system for intercepting biometric authentication data (@ Black Hat Amsterdam)
Tool: Sniffing biometric devices in a domain, as an inline wire tap or proxy device, for ARP poisoning, or as a memory-resident keylogger on a host
Vunerability: Non-Encrypted channel between the biometric scanner and the processing server.
Barrier: Biologger Network Insertion
Mitigation: Encryption of all biometric, user and control data between devices and management servers
(Source)

In the same way Digimarc describes watermarking technology to prevent proliferation of Deepfake news wherein watermarks are embedded in audio and video tracks of video clips of trusted news sources at the time the videos are captured or before they are distributed (Source), biometric liveliness tests could include watermarks tracked by blockchain (see below).

Digimarks system specification (Source) :

- Identify deepfake videos...using unique identifiers and blockchains
- convey information such as *source tracking*, *integrity verification* and *alteration localization*
- serve as standalone software applications or be integrated with other applications

RESOURCES

https://www.biometricupdate.com/202002/advancing-facial-technology-to-fight-identity-fraud-through-liveness-detection

https://www.ecmag.com/section/integrated-systems/deepfakes-new-path-biometric-hacking

https://securityintelligence.com/posts/facial-recognition-deepfakes-and-biometric-pii-preparing-for-a-future-of-faceless-threats/

https://www.techradar.com/uk/news/biometric-technologies-the-key-to-tackling-fraud-and-deepfakes

ZoOm provides biometric security for millions of users worldwide in areas such as on-boarding, KYC, ongoing authentication and age verification. It is used by leading organisations within IAM-IDV, financial services, border security, connected transportation, blockchain-crypto currency, e-voting, among other sectors

FaceTec Inc. FaceTec's patented 3D face authentication software, ZoOm, anchors digital identities, establishing a chain of trust for mobile and web applications requiring certified liveness detection. ZoOm provides biometric security for millions of users worldwide in areas such as on-boarding, KYC, ongoing authentication and age verification.
https://www.sciencedirect.com/science/article/abs/pii/S0969476520300230 (Biometric Technology Today Feb 2020)

Battle Initiatives:
FaceForensics++ and Deepfake Detection Challenge (DFDC) dataset (Hoi Lam, a member of the Institution of Engineering and Technology's [IET] Digital Panel)
Facial recognition cross-referencing increasingly used by video hosting services
techniques are also being explored that implement digital watermarking
https://www.itpro.co.uk/security/357591/why-deepfakes-could-threaten-everything-from-biometrics-to-democracy

Today's AI-driven biometrics are already up to the task of combatting biometric spoofed video presentation. As a deepfake would be treated by an authentication system as a video, if the authentication system is robust to video-based attacks, it should identify what the camera sees as not legitimate or correct.
https://www.sciencedirect.com/science/article/pii/S0969476520300230

from Chat: FID Certification:
https://fidoalliance.org/certification/biometric-component-certification/fido-accredited-biometric-laboratories/

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Which biometric modalities did your group discuss? Check all that apply

[X] Face [ ] Fingerprint [X] Palm [X] Iris/Eye [X] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] Privacy Risks

[X] Accessibility Risks

[X] Inclusion Risks

[X] Diversity Risks

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?

Stewardship, Direction and Policy could be built upon
If YES please provide Contact Information for those who are interested:

- Sunpreet Arora
- Stephanie Schukers
- Daqing (pronounced da ch ing)
- John Mediema, Emmanuel Marasco

Biometrics for Different Ages: Examples, Issues, and Future

Session 6A
Convener: John Callahan
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

The practice of registering individuals' biometric information varies globally. In some places, infant biometric information is not captured until the child is 5 and then is redone when they reach age of majority

https://www.cgdev.org/publication/identification-national-priority-unique-case-peru

Why do we want infant fingerprinting? It would be helpful to ensure vaccine distribution. Paper on infant fingerprints: https://arxiv.org/pdf/2010.03624.pdf

To learn about iris recognition in children: https://ieeexplore.ieee.org/document/9321488

It is difficult to get thumb prints from infants and children. We discussed the challenges of managing children's tendency to have dirty hands, clenched fists and curled fingers which inhibits acquisition of the infant's hand bio-data. Ring lighting vs. scanned -plate type lighting. Sleep was sometimes a good time to capture infant data.

Iris biometrics for kids works well but is challenging to capture in infants. As they get older, it becomes a more reliable option. Note: it has been reported that iris as a measure for older adults degrades over time, but what really happens is that if retina dilation is consistent then the iris does not degrade.

Which biometric modalities did your group discuss? Check all that apply

[x] Face [x] Fingerprint [ ] Palm [x] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**

[x] **Accessibility Risks**

[x] **Inclusion Risks**

[x] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Biometrics and the Role of Open Source

Session 6B
Convener: Jeff Kennedy
Notes-taker(s): Wade & Jeff Kennedy

Please list the key points of your conversation and/or what you would like to share with your colleagues.

One big issue is around how there's no clear incentive for open source communities to form around biometrics needs. Open source projects that start often end up getting blackboxed and sold as products, because there's a clear need and communities tend not to form around the open source code.

There is some clear value in having code be open sourced - namely value in transparency. It makes what you're doing more trustworthy, because people can see what your algorithm does. It also provides a mechanism for proving that you are good at DEI - because it can be run against any dataset that you please,

not just the one that the company uses. Additionally, if your company goes bankrupt, your customers could conceivably pick up where you left off and they won't be in trouble because of you.

Should the open source initiative be more robust…?
Inclusion of privacy rights groups

Chain of processing and analyzing

from chat: http://www.openbiometricsinitiative.org/
http://www.openbiometricsinitiative.org/about.html

http://openbiometrics.org/

OpenABIS finds its roots in the need of an ABIS for ID PASS Digital Identity Solution, our sister project which enables governments and humanitarian organizations to issue and verify a decentralized, private, trusted and recoverable form of identity t
https://idpass.org/

https://www.nist.gov/itl/iad/image-group/products-and-services/image-group-open-source-server-nigos
https://www.idiap.ch/software/bob/docs/bob/bob.bio.base/v4.1.1/index.html

Android

Biometrics are measured with the Imposter Accept Rate (IAR) and Spoof Accept Rate (SAR).
https://source.android.com/security/biometric
https://source.android.com/security/biometric/measure#strong-weak-unlocks
Open Source Ref system (2008)
https://www.academia.edu/14382781/Open_Source_Reference_Systems_for_Biometric_Verification_of_Identity
Open Source Java Framework for Biometric Web Authentication Based on BioAPI Amit Sharma
https://www.academia.edu/9334758/An_Open_Source_Java_Framework_for_Biometric_Web_Authentication_Based_on_BioAPI

(PoC) open source software is developed for realizing a privacy preserving voice verification prototype based on slice-based architecture (Source)

Which biometric modalities did your group discuss? Check all that apply

[X] Face [X] Fingerprint [ ] Palm [X] Iris/Eye [X] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**

[X] **Accessibility Risks**

Note: Transparency needed for the two risk items below

[X] Inclusion Risks

[X] Diversity Risks

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?

There is a strong need to apply pressure to existing providers of biometrics solutions (matchers, verifiers, testers, storage providers) to open source their products. We hope we can get some privacy rights groups to take up the cause and get the word out and come up with good ways to apply such pressure.

If YES please provide Contact Information for those who are interested:

You can contact Jeff at jeffk@kiva.org. By no means am I an expert in this area, just someone who wants to see good things happen!

Friday March 12 / Sessions 7 - 9

The Privacy, Accessibility, Inclusion and Diversity (PAID) framework for Biometric Technologies

Session 7A
Convener: John Callahan
Notes-taker(s): Chris

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Chat notes:

We see eye to eye, so to speak

This table is brilliant

Risk, Trust, and Bias: Causal Regulators of Biometric-Enabled Decision Support

Biometrics and biometric-enabled decision support systems (DSS) have become a mandatory part of complex dynamic systems such as security checkpoints, personal health monitoring systems, autonomous robots, and epidemiological surveillance.

R-T-B Casual Landscape:
https://www.researchgate.net/profile/Svetlana-Yanushkevich/publication/343498507/figure/fig3/AS:921734081441803@1596769938358/The-R-T-B-causal-landscape.ppm

maybe could adapt this GDPR model of risk influences:
https://bizzdesign.com/wp-content/uploads/2017/01/Blog-GDPR-Compliance-image1.png

tool fatigue

@Eris: yes cognitive load

Tech change is similar to large real world change. It (IT) happens. It is much like the frustration of a new car and/or home (light switches).

I had gotten frustrated at my location changes in my weather app when the developer had to do it once lol

great prez John

Agreed, great presentation! Any chance we could get a link to those slides?
+1 on the slide request

+1 plus Johns contact info

Biometric Information Privacy Act (BIPA), the California Consumer Privacy Act (CCPA) demonstrates how legislators will also turn to other ways to impose requirements and restrictions over biometrics (Illinois)

https://www.blankrome.com/publications/analyzing-ccpas-impact-biometric-privacy-landscape

https://www.law.com/legaltechnews/2020/10/14/analyzing-the-ccpas-impact-on-the-biometric-privacy-landscape/

+1 on slides

https://www.bayometric.com/risks-storing-biometric-data/

Stephanie is next, then Tim

Tim, then Eric, then Dan B.

10:44:17 From Wade (bioMetricity) to Everyone : PoC 2020

4 Major Attacks: 2D and 3D masks, replay attacks and coercion
> National ID cards found to be the most frequently defrauded documents, the report adds, citing the Indonesian, Italian and Polish ID cards as the most frequently attacked

https://www.biometricupdate.com/202012/onfido-report-notes-new-biometric-fraud-trends-and-id-fraud-spike-in-covid-19-era
https://onfido.com/resources/reports-whitepapers/identity-fraud-report-2020

Legacy Attacks

PoC 2008
Concept: "Biologging" (Matthew Lewis, British security researcher) system for intercepting biometric authentication data (@ Black Hat Amsterdam)
Tool: Sniffing biometric devices in a domain, as an inline wire tap or proxy device, for ARP poisoning, or as a memory-resident keylogger on a host
Vunerability: Non-Encrypted channel between the biometric scanner and the processing server.
Barrier: Biologger Network Insertion
Mitigation: Encryption of all biometric, user and control data between devices and management servers

Like Infant biometrics :)

they are very very keen on doing this throughout the developing world.

Excellent points...

Hello Attack: Persistent Active Directory backdoor (Michael Grafnetter, IT security researcher and trainer for CQURE and GOPAS)
https://www.blackhat.com/eu-19/briefings/schedule/index.html#exploiting-windows-hello-for-business-17260

Vunerability: Vector in a security-critical AD attribute called msDS-KeyCredentialLink, (store data related to Windows Hello, FIDO2, or BitLocker Drive Encryption). It holds references to devices that users register with Active Directory for authentication. If someone registers a notebook or YubiKey with WHfB, data is logged with msDS-KeyCredentialLink.

https://www.darkreading.com/cloud/windows-hello-for-business-opens-door-to-new-attack-vectors/d/d-id/1336396

^ Windows Hello for Business (WHfB) was introduced in Windows 10 and Windows Server 2016 to bring password-less authentication into Active Directory-based environments

Systems: Microsoft, Active Directory, or Azure Active Directory account
Credential: biometric or PIN. WHfB is built on top of Industry Standards: Kerberos PKINIT, JWT, WS-Trust, or FIDO2,
Cryptographic Mechanisms: TPM key attestation or token binding

+10 - i don't want to live in a world ruled by laws, i want to live in a world ruled by people *guided* by laws

10:57:34 From Wade (bioMetricity) to Everyone : @Eric: good point keep the human in the ODDA loop as they are talking in AI ethics within military

10:58:49 From Eric Welton (Korsimoro) to Everyone : @Ushnish - I embody that concern ;)

Regarding making the world into an operating system: Can you create an operating system to meet real world is key point too. The more we look to align digital with analog, the more fierce the challenge. Digital is not organic and the HumanOS does not have"0" and "1" processors. Much more gray area there than digital can't well mimic.

Thx!

Thanks for the great presentation and for hosting this conversation!!

11:01:28 From Tim Newman to Everyone : Thank you!

Which biometric modalities did your group discuss? Check all that apply

[x] Face [x] Fingerprint [ ] Palm [x] Iris/Eye [x] Voice [x] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[x] **Privacy Risks**

[x] **Accessibility Risks**

[x] **Inclusion Risks**

[x] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

Biometric Incident Response

Session 7E
Convener: Wade Bittle
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Crucial Breach Verticals: Health, Banking

Definitions: Operational Environment, Data Collection
" Tools Do Not Create Intelligence, Analysts Create Intelligence"

Incident Response Stages: Preparation, Detection & Identification, Evidence & Acquisition, Time Critical Analysis

Focus on: Protecting Template Storages and Trust Registers, as well as the verification blockchain

https://lifars.com/2020/05/biometrics-and-cybersecurity

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[ ] **Privacy Risks**
[ ] **Accessibility Risks**
[ ] **Inclusion Risks**
[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

How does SSI, FIDO, Physical and non-physical Biometrics, Identity and Authentication all fit together, for privacy, security and Compliance?

Session 8A
Convener: Brian Clinkenbeard
Notes-taker(s):

Please list the key points of your conversation and/or what you would like to share with your colleagues.

CSET = https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[ ] **Privacy Risks**
[ ] **Accessibility Risks**
[ ] **Inclusion Risks**
[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

DID (what is it) and how did Biometrics come (and go) in w3c/did-core

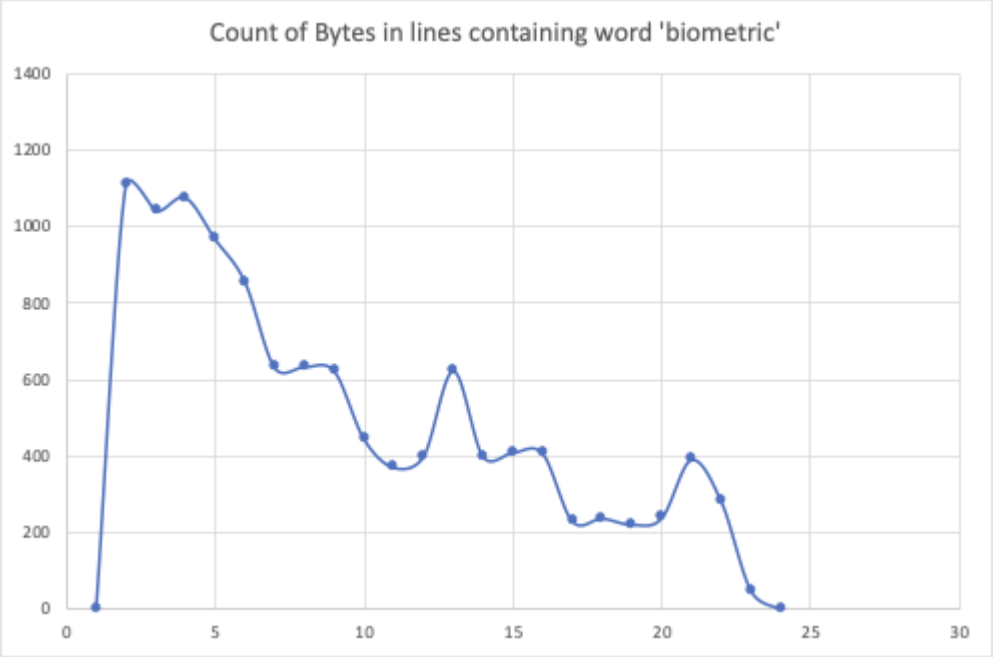
Session 9A
Convener: Eric Welton
Notes-taker(s): Eric Welton

Please list the key points of your conversation and/or what you would like to share with your colleagues.

- Discussion of DIDs
- Concern that "the only way to understand DIDs is to be in the community for years"
- Looked at various commits and traced the word 'biometric' in the w3c/did-core spec

Count of bytes in lines containing word 'biomeric' (e.g. grep biometric | wc) by date

```
   0 Mar 12 15:17 checks.2017-10-28 13:06:14 -0400
1110 Mar 12 15:17 checks.2017-11-05 06:27:14 -0500
1041 Mar 12 15:17 checks.2017-11-30 15:33:21 -0500
1076 Mar 12 15:17 checks.2018-01-15 09:18:02 -0500
 968 Mar 12 15:17 checks.2018-01-30 15:33:40 -0500
 856 Mar 12 15:17 checks.2018-02-08 20:26:09 -0500
 632 Mar 12 15:17 checks.2018-05-16 11:29:07 -0400
 634 Mar 12 15:17 checks.2018-07-09 16:54:51 -0400
 623 Mar 12 15:17 checks.2019-02-05 21:25:25 -0500
 446 Mar 12 15:17 checks.2019-05-31 15:37:08 +0200
 371 Mar 12 15:17 checks.2019-08-06 18:57:54 +0200
 400 Mar 12 15:17 checks.2019-08-08 22:56:00 +0200
 623 Mar 12 15:17 checks.2019-09-18 02:07:50 -0600
 400 Mar 12 15:17 checks.2019-09-23 14:44:00 -0600
 410 Mar 12 15:17 checks.2019-10-19 02:03:12 +0400
 408 Mar 12 15:17 checks.2019-11-26 21:37:31 -0500
 231 Mar 12 15:17 checks.2020-02-12 19:37:34 -0500
 238 Mar 12 15:17 checks.2020-05-04 11:33:27 -0400
 222 Mar 12 15:17 checks.2020-05-28 21:36:20 -0400
 239 Mar 12 15:17 checks.2020-05-28 21:41:36 -0400
 391 Mar 12 15:17 checks.2020-06-07 22:12:54 -0400
 283 Mar 12 15:17 checks.2020-06-22 11:13:41 -0400
  50 Mar 12 15:17 checks.2020-12-01 10:17:41 -0500
   0 Mar 12 15:16 checks.2021-01-31 16:21:28 -0500
```



2017-11-05 DID-Core Examples

Introductory Paragraph

Decentralized Identifiers (DIDs) are a new type of identifier intended for verifiable digital identity that is "self-sovereign", i.e., fully under the control of the identity owner and not dependent on a centralized registry, identity provider, or certificate authority. DIDs resolve to DID Objects — simple JSON documents that contain all the metadata needed to interact with the DID. Specifically, a DID Object contains at least three things. The first is a set of mechanisms that may be used to authenticate as as a particular DID (e.g. public keys, **pseudonymous biometric templates**, etc.). The second is a set of authorization information that outlines which entities may modify the DID Object. The third is a set of service endpoints, which may be used to initiate trusted interactions with the identity owner. Each DID uses a specific DID method, defined in a separate DID method specification, to define how the DID is registered, resolved, updated, and revoked on a specific distributed ledger or network.

Example Guardian-Managed DID Description

Following is a second example of a DID Description that describes the DID above. In this case the DID Description describes a dependent—an entity who is not currently in a position to control the private keys for this identity. This DID Description was created by a guardian—a separate identity owner with its own DID that serves as a trustee for the dependent. Note that while this DID Description asserts a set of service endpoints, it does not yet contain a set of key descriptions because the dependent does not yet have its own set of private keys.

```
{
  "@context": "https://example.com/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authorization": [{
    // this entity is a guardian and may update any field in this
    // DID Description using any authentication mechanism understood
    // by the ledger
    "capability": "UpdateDidDescription",
    "entity": "did:example:zxyvwtrkpn987654321"
  }],
```

```
  "credentialRepositoryService": "https://vc.example.com/abcdef",
  "authenticationCredential": [{
    // this biometric can be used to authenticate as DID ...fghi
    "id": "did:example:123456789abcdefghi/biometric/1",
    "type": "PseudonymousBiometricTemplate2017",
    "owner": "did:example:123456789abcdefghi",
    "biometricService": "https://example.com/authenticate"
    "biometricTemplateShard": "Mjk4MzQyO...5Mzg0MDI5Mwo="
  }]
}
```

Which biometric modalities did your group discuss? Check all that apply

[ ] Face [ ] Fingerprint [ ] Palm [ ] Iris/Eye [ ] Voice [ ] DNA
[ ] Behavioral
[X] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[ ] **Privacy Risks**
[ ] **Accessibility Risks**
[ ] **Inclusion Risks**
[ ] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

COVID-19 Focus: How has the pandemic impacted biometrics? And what are ethical concerns related to health data collection?

Session 9D
Convener: Tim Newman and Marilene Oliver
Notes-taker(s): Tim Newman

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Framing questions from Marilene: using medical can data to create artwork; They download open-source, anonymized data sets, but they can now be traced back to facial recognition in the data set -- there are ways to anonymize, but that has ethic questions too; WIth VR hardware itself, because there is eye tracking, there could be iris scanning as well as gait tracking -- they were using Oculus but to continue using it, you sign in with FB which collects biometric data -- there's potential for harm there; Once you've got biometric authentication, are all these data entities joined and will, for example, bank and health providers want that linked data; Another question is about "trust" generally

Framing questions from Tim:

- What biometric tools are being developed that respond specifically to COVID-19?
- What are the ethics concerns and implications of this technology?
- How has the pandemic impacted the biometric field generally beyond just new technology that responds specifically to COVID-19?

Notes:

- Marilene: With Oculus and other VR technology, you have to consent to sharing your biometric data;
- John Callahan: Kaliya has a role in COVID Credential Initiative; from a person perspective, resisted VR, but son wanted one so he chose HTC Viva since it doesn't require FB login;
- Jeff O: it's a double-edge blade; being anywhere near Facebook makes me reticent; the ecosystem re VR is complicated, so it's just a risk analysis of what to choose; in talking with younger people: imagine yourself in a big open field, as you connect with others, bites of grass are taken away and in the future, that grass diminishes, so understand what you are giving up;
- Wade: when it comes to image data, you can de-identify, but it can be complex based on what you are doing; Could there be a private identifier with a custodian who could decrypt data?
    - Marilene: anonymizing works to some extent, but there's potential for it be reversed if there's someone with motivation strong enough;
    - Alex Jonsson: Re question of insurers getting access and then denying care, that should be illegal in the US and Canada; There's 16 PII markers and depending on the data set, they randomly take off or fill in inputted value and then it becomes too hard to correlate someone; More of a concern with facial recognition, but some cities are starting to address that;
- Katrina Ingram: works with Kaliya on the COVID project; Other risks: there is potential for us to be mined for our data and then repackaged in a way that mirrors subprime mortgage packaging; The data can be packaged and resold; The other
- Alex: data brokers are part of the B2B space but maybe not as much health data although it's a bit of a Wild West among nonprofits that are major health providers;
- John Callahan: re COVID, for public health reasons and tracing, there are reasons to be concerned about the privacy concerns there and it's a tricky landscape; my opinion has been for public health

reasons, it can be helpful, but for privacy reasons, even with HIPPA, etc there are concerns; And if there are a small number of participants, is it effective -- especially with the tradeoff of privacy?

- Alex: contact tracing is top down and can be ineffective (for example, it's gotta work fast for effectiveness)
- Jeff Kennedy: had a lot of conversations with people about expectations about when they'll return to the office; ex: when people get vaccinated, do I have to go to the office and vice-versa can employer compel people to reveal - and what kind of precedent does this set for other health conditions?
- Jeff O: intrigued about volumetric data for the purpose of art;
- Marilene: there are a lot of open source data some with CC and some just for research, etc; they're also making tools to help people make VR out of medical scans - which has a lot of great potential but also potential for harm; especially concerned if biometric authentication combines all this data;
- John Callahan: I could see some benefits for this VR tech being used for training for medical students, for example; Wiht cadaver training, there are a lot of ethics standards - does that exist for this kind of data and work?
- Marilene: this data would have been collected through studies that have ethics standards and agreements; One question is when tech is evolving so quickly, when people consented some of the tech the data is being used for may not have been around at the time;
- Katrina: medicine has a lot of parallels here and ethic conversations took hundreds of years; we're relying on a bioethics model when it comes to this data;
- Marilene: already we're finding there are different codes in different areas like GDPR says people should have access to the medical scan while that's not a right in Canada; Should we have international codes?
- Jeff O: We're really needing a Digital Hippocratic Oath
- Katrina: there's a lot of conversation about "can you really give consent in an employee relationship" and is the appropriate place to negotiate data consent in the empoyee contract
- Kaliya: re verifiable credentials allow packaging up of info from an issuer to give to an individual who can share the verifiable credential with others - you would be able to see if the credential has been tampered with; this is broad and open as opposed to others that focus on one specific type of credential; a year ago, people working on this saw how it might play a role in the sharing of health info re pandemic (ex: digital version of the yellow card?); It's an open community and anyone can join Slacks and meetings; last week they were talking about how to turn it into QR code, etc to make it accessible; airline industry and governments are looking at what travel looks like coming back; still a lot of questions -- for decades, there have been international travel protocols around things like this; Any proprietary app should raise concerns - ex: there's a closed loop one that tracks tests over time and then is used as a basis for you to access university, etc; There's a Microsoft initiative where they extract data from health records and then you're supposed to trust their system; Good Health Pass is more aligned
- Alex: is there a benefit here? You used to be able to charge for asking for data;
- John Callahan: even before COVID, there was an IEEE open source gitlab repository; their use case was wanting to replace the paper yellow card; IEEE has a biweekly group talking about this stuff;
- Marilene: when folks share code, do you also share ethics considerations?
- Alex: probably depends on industry; medical industry might be thinking and sharing that, but maybe not an average app developer

Chat log:
Thanks TIM! :)
My understanding is that regarding having data gathered from behavior, I understand mobile devices give off upwards of 250-300 data points regarding "behavioral analytics" as another concern.

https://www.biometricupdate.com/202103/governments-weigh-use-of-biometric-vaccine-certificates-vision-box-iproov-and-evernym-positioned
https://www.biometricupdate.com/202103/uk-care-facility-trials-fingo-vein-biometrics-for-covid-digital-health-pass

I work as the Ecosystems Director at the CoVID-19 Credentials Initiative - working on leveraging verifiable credentials for sharing test results and vaccine status

mmmm...you would understand the details
https://www.igi-global.com/chapter/behavioural-data-collection-using-mobile-phones/113201

https://healthtechmagazine.net/article/2019/12/biometrics-healthcare-how-it-keeps-patients-and-data-safe-perfcon

about Heatlh Custodians

"circle of care" is not a defined term in the Personal Health Informa-tion Protection Act, 2004 (PHIPA)

https://www.ipc.on.ca/wp-content/uploads/Resources/circle-of-care.pdf

Personal information is defined differently between jurisdictions and it could have an impact on the ISA.Some professional/employee information is not considered personal information in some jurisdictions while it is in other jurisdictions. Most privacy legislation applies to recorded personal information but some privacy legislation applies to recorded and non-recorded personal information.

https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html

https://www.ipc.on.ca/wp-content/uploads/2019/09/2019-08-09-datashare-web.pdf
^ Intro to Data Sharing rules

Plenty of time for both Jeff's!

recent article related to workplace rights/surveillance in Canada -
https://www.theglobeandmail.com/business/commentary/article-algorithms-are-increasingly-treating-workers-like-robots-canada-needs/

Thanks, Katrina!

if being COVID tested is a workplace safety issue, it potentially mirrors drug testing. Could be a case made to say this is a condition of employment for workplace safety.

That's a good point, this is sort of a second precedent then.
Or rather, it has that precedent and so there may be few arguments against it.
Me to Everyone (3:31 PM)

This is all interesting!

https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

)passing House Bill 678, the Legislature recognized that many transactions that now require a password or some other form of identification would utilize biometric technology

https://www.law.uh.edu/healthlaw/perspectives/Privacy/010824Biometrics.html

S.1842 - Protecting Personal Health Data Act
116th Congress (2019-2020)

https://www.congress.gov/bill/116th-congress/senate-bill/1842/text?q=%7B%22search%22%3A%5B%22personal+data+health%22%5D%7D&r=1&s=1

Changes to scope, nature and purpose are particular ethical issues.
Wade (bioMetricity) to Everyone (3:36 PM)
Semantic Parametric Reshaping of Human Body Models. In 3DV Workshop on Dynamic Shape Measurement and Analysis, 2014. Dataset The dataset contains about 1500 registered male and female meshes with point-to-point correspondences respectively. Each mesh has 12500 vertices and 25000 facets. The data is derived from the CAESAR dataset.

https://graphics.soe.ucsc.edu/data/BodyModels/index.html

Digital Hypocritic Oath concept
Wade (bioMetricity) to Everyone (3:40 PM)
A Global Review of Publicly Available Datasets

140 unique datasets, only 94 were open access from which the raw data could be downloaded. 27 datasets were categorised as open access with barriers, from which data could not be downloaded. 19 datasets had regulated access (12 requiring licensing agreements, six requiring an ethical committee or institutional approval, and one requiring a payment of £2250

https://www.sciencedirect.com/science/article/pii/S2589750020302405

https://medicalfuturist.com/why-an-upgraded-hippocratic-oath-is-needed-in-the-digital-era/

https://clayholderman.health/blog/whathappenedtotrust

https://www.chlt.org/hippocrates/oath/page.0.a.php

https://onezero.medium.com/those-covid-19-temperature-scanning-kiosks-use-scary-powerful-facial-recognition-8cc8ada0c595

https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/

https://globalnews.ca/news/7687737/covid-vaccine-passports-eu-canada/

^ re: wired article
dang
GoSafe, could scan foreheads for elevated temperatures and detect when students aren't wearing masks. It also came with a bonus: "top-of-the-line" facial recognition,

https://www.covidcreds.org/

A view of privacy in context - not just about access and control, but situational - https://www.ethicallyalignedai.com/post/book-review-privacy-in-context

^ wired article
Facial recognition is not a requirement for back to school pkg
"equipping schools with facial recognition during a crisis normalizes the technology with little debate or public input."
(Shobita Parthasarathy)

https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/

@wade- exactly - things are brought in with little discussion , get normalized and have far reaching implications

Thanks for references!
John Callahan to Everyone (3:54 PM) https://opensource.ieee.org/p2418-6/verifiable-vaccinations

@kaliya what is the article re: VCI

@Katrina: yes it can work like that
our guard is down and biologically speaking because of a low-grade background trauma, as well as COVID fatigue - people are ready to jump including policy makers.

The Verifiable Credential Flavor paperobliquely critiques VCI
they are JSON-JWT focused it is the least privacy preserving option for VCs

Which biometric modalities did your group discuss? Check all that apply

[X] Face [ ] Fingerprint [ ] Palm [X] Iris/Eye [ ] Voice [X] DNA
[X] Behavioral
[ ] Other (please specify all) _____

Were any of the following Risks considered? Check all that apply and add any relevant notes about the discussion.

[X] **Privacy Risks**
[X] **Accessibility Risks**
[X] **Inclusion Risks**

[X] **Diversity Risks**

NEXT STEPS? Will you take any Next Steps and/or continue this conversation?
If so, can other's from the workshop join?
If YES please provide Contact Information for those who are interested:

As a result of attending #TBE2021……

As a result of attending the Thoughtful Biometrics Workshop, I'll share my notes and everything I learned from you all with my colleagues to inform our thinking and research on these topics

I am going to put my information of Deepfakes, Biometric and Incident Response in a slide deck and you gents and ladies will be the first to access it Hopefully posted to the documents if they're around

As a result of attending the Thoughtful Biometrics Workshop, I learnt about SSI and the importance of decentralizing biometric data

* i am re-invigorated to find an automaton f=gen(IBV,private-key,thresh) such that f(doc,CBV)=enc(doc,private-key) where f is FHE.

expanded my concepts of self-sovereignty, DDI, SSI, made a whole bunch of friends and that there is good hiking trails in Thailand

...I learned about deeper aspects of biometrics. I make contacts with similar questions. I was amazed by the body of knowledge and sharing.

As a result of attending TBW'21, it is clear to me that the chain-of-trust from identity verification through the holder of a credential (like FIDO) using the bound local authenticator to the verifier/relying party is critical to success

As a result of attending the Thoughtful Biometrics Workshop, I feel significantly more prepared to implement a secure system using biometrics authentication.

As a result of attending the Thoughtful Biometrics Workshop...I am better able to discuss and communicate thoughts and ideas concerning this data type and its preferred ethical usage of such.

As a result of attending the Thoughtful Biometrics Workshop, I came out with at least as many questions as answers ;) In truth, I was inspired by the well-meaning people in this space!

I learned that biometrics are probabilistic rather than deterministic of identity and therefore a gray area that has multiple dimensions that need to weigh in to their approved/secured use

As a result of attending the Thoughtful Biometrics Workshop I feel overwhelmed at how complex it is and hope we can keep the future simple

Where the word DID is used Phonetic DeyeD may clarify that I DID use a DeyeD where DID, may confuse? Great learns!

THANK YOU TO THE SPONSOR!

Thank you so much to the folks who organized and facilitated!

Thank you to all.

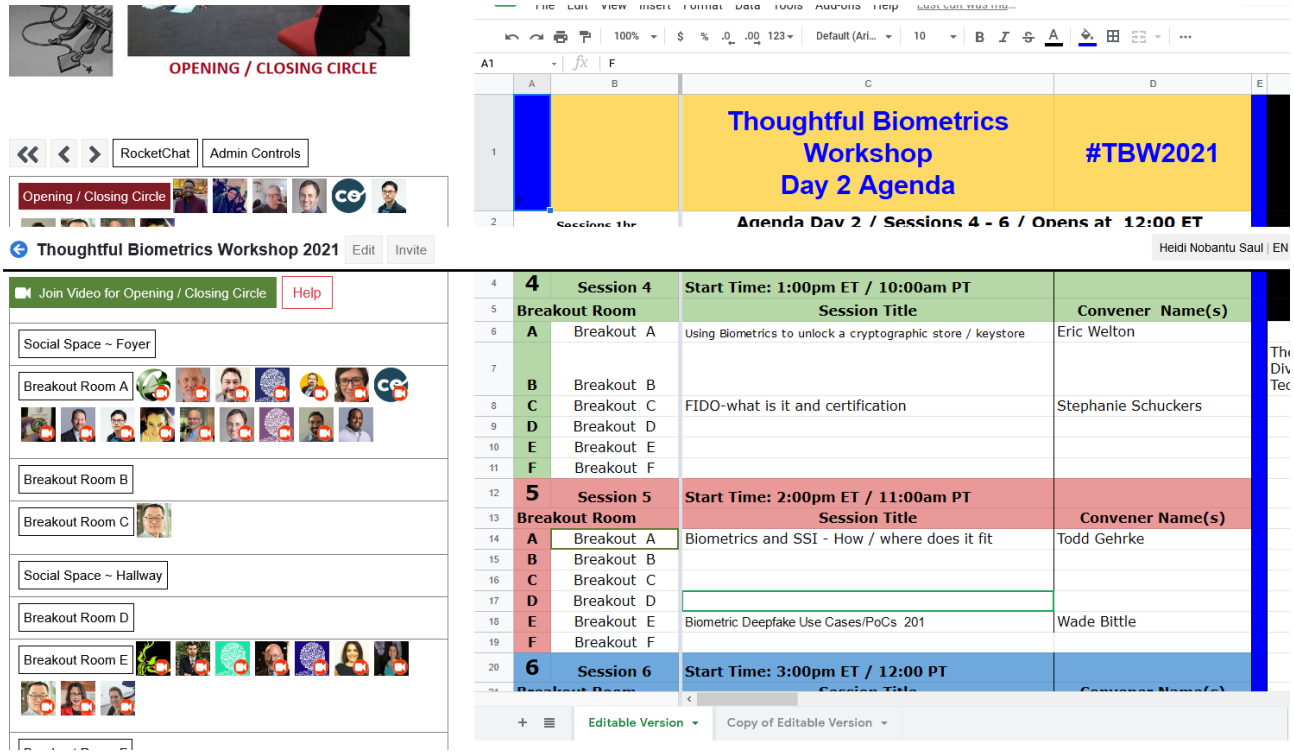
Heartfelt thanks to everyone involved with organizing this inaugural event!

: love your word play

Thank you all for this workshop, great to meet you all. Hope to see you again soon, Marilene

Yes! The spacing was nice.

Great format!



For More Information about

The Thoughtful Biometrics Workshop

and a possible repeat event in 2022

https://thoughtfulbiometrics.org/