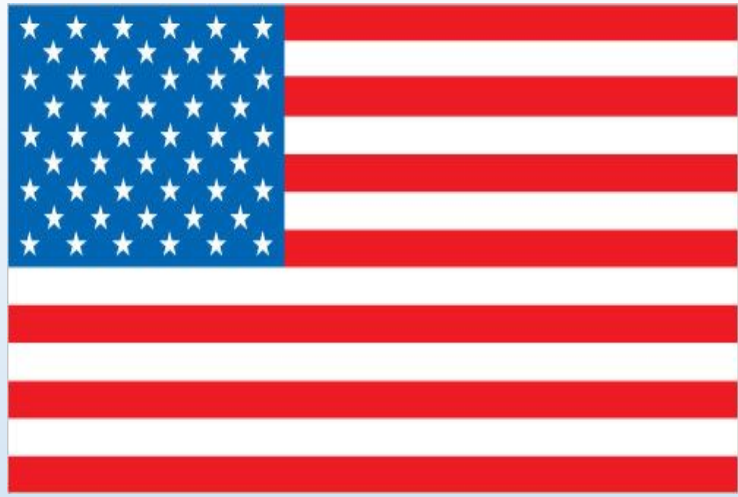
Human Nature, Artificial Intelligence and the Internet of Things: Challenges for Human Rights from International Criminal Law to Personal Autonomy and Inviolability

Perm State National Research University
4 June 2020

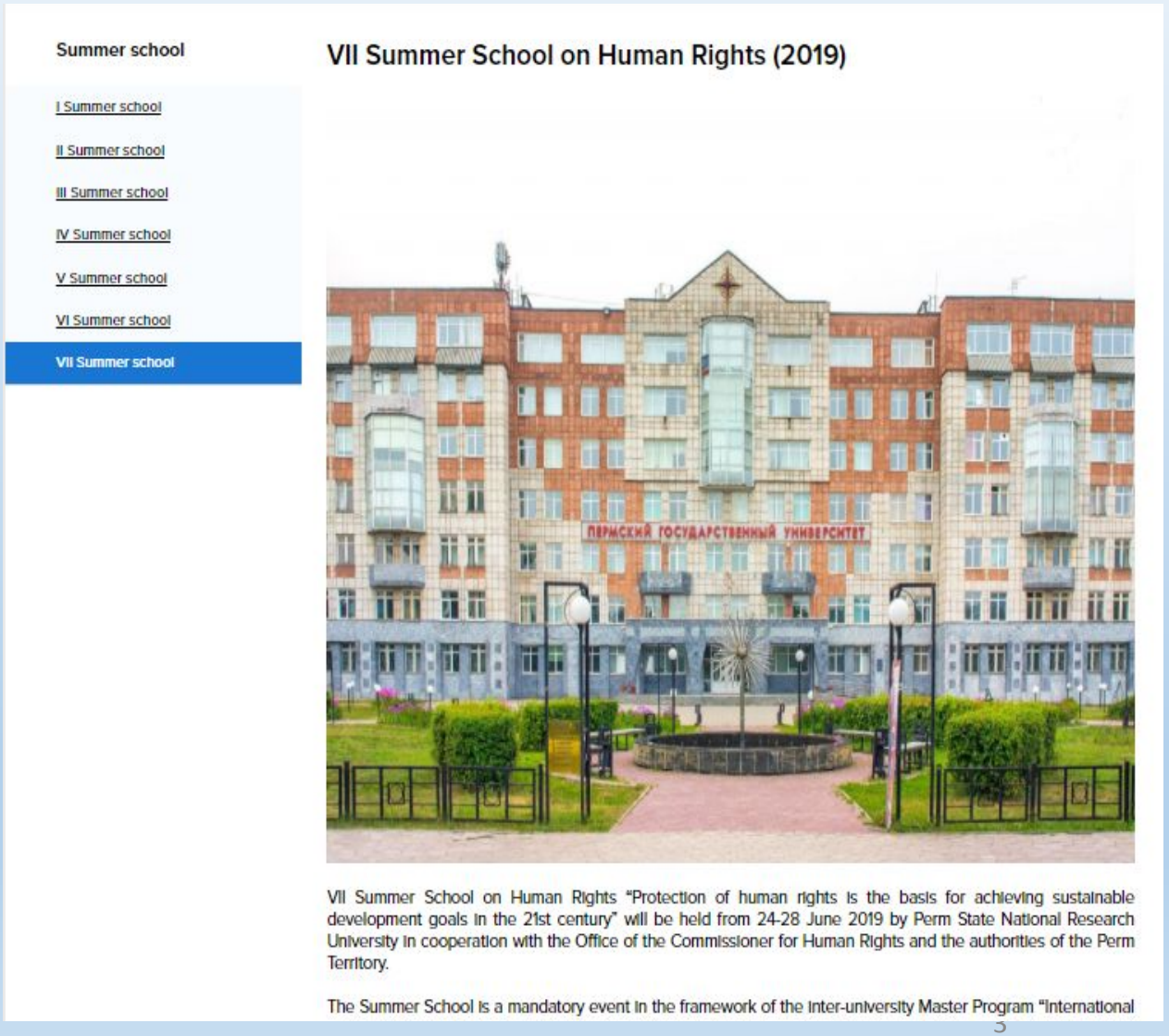
PGU– UofL Collaborations



What will come?

- Michael Losavio, Kentucky
- Kareem Codrington, Antigua
  - Department of Criminal Justice, University of Louisville, Kentucky, USA

Thanks to OHCHR and PGU



Abstract-*Human Nature, Artificial Intelligence and the Internet of Things: Challenges for Human Rights from International Criminal Law to Personal Autonomy and Inviolability*

- In this *interactive* session we discuss the growth of the International Regime of Criminal Justice and the impact of the Internet of Things and Artificial Intelligence on people throughout the world.
- We analyze and identify the benefits and detriments in
  - The evolving human rights regime of international criminal justice and how it may or may not protect people in the world
  - The impact of the Internet of Things on human rights and ethics through its distribution sensing and connectivity on the lives of others, and
  - The impact of Artificial Intelligence and Predictive Analytics on the freedoms and liberties of people everywhere through unprecedented and sometimes unexplained inferential judgments on those people.

WSJ
1 June 2020

.

WSJ PRO

CYBERSECURITY

Cyber Daily: Human-Rights Groups Want Law Enforcement to Do More to Stop Hospital Cyberattacks

By Kim S. Nash

Welcome back. Opportunistic cyberattackers continue to target hospitals during the coronavirus pandemic. The International Committee of the Red Cross and other human-rights groups are urging law enforcement to move against these hackers, WSJ Pro's Catherine Stupp and David Uberti report. "What we're seeing at the moment are still indications of how devastating it could be," said Cordula Droege, chief legal officer at the ICRC.

SHARE

TEXT

Human-Rights Groups Ask Police to Hunt Hackers Attacking Hospitals

As the coronavirus pandemic wears on, cyberattackers continue to strike

United Nations High Representative for Disarmament Affairs Izumi Nakamitsu addresses the U.N. Security Council in February.

PHOTO: BEBETO MATTHEWS/ASSOCIATED PRESS

By Catherine Stupp and David Uberti
June 1, 2020 5:30 am ET | WSJ PRO

The International Committee of the Red Cross and other human-rights groups are urging

TOP NEWS

Cybersecurity Startups Feel Pinch on Funding and Sales

RELATED NEWS

Human-Rights Groups Ask Police to Hunt Hackers Attacking Hospitals

As States Reopen, the Boss Wants to Know What You're Up To This Weekend

Lawmakers Urge More

The goals- a.k.a. *what's in this for you?*

- identify the challenges
  -
  -
  -
- Identify the benefits
  -
  -
  -
- apply techniques to protect the rights and the benefits of us in this new, brave world
  - ❖
  - ❖
  - ❖

Did I mention this session is interactive?

Breakouts will be part of this

Please feel free to interrupt!

- You may comment via your microphone
- You may chat via the videoconferencing chat tool
- You may email me a michael.losavio@louisville.edu
- You may text me via WhatsApp at +1 502 417 4970 (*but possible delay*)

FIRST: let me know about you, to tune our discussion

- Please let me know
  - your interests and
  - what you would like out of this discussion

- By Zoom chat
  - Or email michael.losavio@Louisville.edu
  - Or text +1 502 417-4970, telco or WhatsApp

Ethics and Human Rights?

- They are harmonized in the evolution of our values.
- Tthics may serve as an early warning of the risk of injuries. And legal liability.
- We examine how consideration of ethics in may warn of human rights and social-legal-technical conflicts.

Founders- Ethics in Medical Science

Mudrov Matvei Yakovlevich (d 1831), Boris Yudin (d. 6August 2017_

-

ICT & Ethics is Evolving:

The **Menlo Report:** Ethical Principles Guiding Information and Communication Technology Research August 3, 2012
https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf

- The Menlo Report…
- proposes a framework for ethical guidelines for
  - computer and
  - information security
  - research
- based on the principles set forth in the 1979 Belmont Report…
- …

- new challenges resulting from interactions between humans and communications technologies. …

- …ICT research contexts contend with
  - ubiquitously connected network environments,
  - overlaid with varied, often discordant legal regimes and social norms. …

- Consider history of:
  - traditional human subjects research, and the
  - landscape of ICT research stakeholders.

- four core ethical principles, the three from the Belmont Report
  - Respect for Persons,
  - Beneficence, and
  - Justice (Belmont) with
  - an additional principle *Respect for Law and Public Interest*.

- Goal: propose standard methods for ICT research for:
  - identification of stakeholders and informed consent;
  - balancing risks and benefits;
  - fairness and equity; and
  - compliance, transparency and accountability, respectively.
    - these principles and applications can be supported by outside oversight and internal self-evaluation tools.

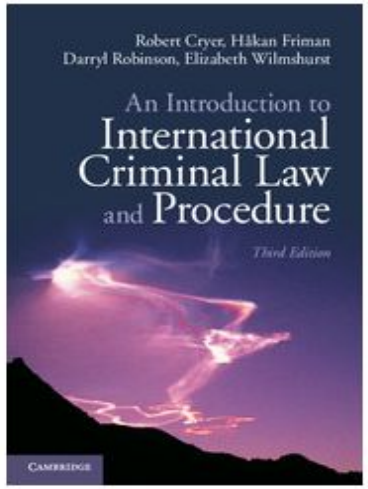
Part 1 – Human Nature

- International Criminal Justice deals with the worst things we do
- It's focus in on the generally agreed upon prohibitions on mass human misconduct
- These are the most terrible manifestations of human nature
  - Trigger warning – we may discuss some of these terrible things

Recommendation: Cryer, Friman, Robinson & Wilmshurst, *An Introduction to International Criminal Law and Procedure* , 3rd Edition at https://www.cambridge.org/core/books/an-introduction-to-international-criminal-law-and-procedure/1CEAA618D0EC98E22498D65103D4AFEC, accessed 2 June 2020

An Introduction to International Criminal Law and Procedure

Search in th



Free access to HTML textbooks is now available again and is being offered direct to Higher Education institutions. Access will be automatic if your institution has been given access. If you don't have access, details for librarians to action are available on this page.

Textbook

Get access Cited by **45**

3rd edition

Robert Cryer, *University of Birmingham* , Håkan Friman, *University College London* , Darryl Robinson, *Queen's University, Ontario* , Elizabeth Wilmshurst, *University College London*

Publisher: Cambridge University Press
Online publication date: May 2018
Print publication year: 2014
Online ISBN: 9781107588707
DOI: https://doi.org/10.1017/CBO9781107588707

International Criminal Justice?

Focus 1: *International and* transcending purely domestic jurisdiction

Focus 2: *Individual accountability* for heinous acts in violation of international law

the meaning of international criminal law

- Traditionally international law addressed the rights and obligations of States
- Criminal law traditionally addressed punishment for conduct by individuals as a fundamental aspect of domestic police power
- These would seem inherently incompatible,
  - yet with the evolution of treaty law and international/transnational norms a regime of international criminal law punishing individuals for their actions through international mechanisms has evolved.

The Sources of International Criminal Law

- War crimes-"the laws and customs of war“
- Genocide and crimes against humanity
- Aggression of one state against another
- From the International Criminal Tribunal for the former Yugoslavia (ICT Y) *Tadic* case
  - A State-sovereignty-oriented approach has been gradually supplanted by a human-being-oriented approach… International law, while of course duly safeguarding the legitimate interest of States, must gradually turn to the protection of human beings. Opinion of 2 October 1995, paragraph 97

Consider…

Rohingya crisis: The Gambia accuses Myanmar of genocide at top UN court

4 hours ago

Asia migrant crisis

The small west African nation of The Gambia has filed a lawsuit at the UN's top court formally accusing Myanmar of genocide against Rohingya Muslims.

It was filed at the International Court of Justice (ICJ), which normally rules on

INTERNATIONAL COURT OF JUSTICE

APPLICATION INSTITUTING PROCEEDINGS
AND
REQUEST FOR PROVISIONAL MEASURES

REPUBLIC OF THE GAMBIA

v.

REPUBLIC OF THE UNION OF MYANMAR

11 November 2019

APPLICATION INSTITUTING PROCEEDINGS AND REQUEST FOR PROVISIONAL MEASURES

To the Registrar of the International Court of Justice,

The undersigned, being duly authorized by the Government of the Republic of The Gambia, states as follows:

1. In accordance with Articles 36(1) and 40 of the Statute of the Court and Article 38 of the Rules of Court, I have the honour to submit this Application instituting proceedings in the name of the Republic of The Gambia ("The Gambia") against the Republic of the Union of Myanmar ("Myanmar"). Pursuant to Article 41 of the Statute, the Application includes a request that the Court indicate provisional measures to protect the rights invoked herein from imminent and irreparable loss.

I. Introduction

2. This Application concerns acts adopted, taken and condoned by the Government of Myanmar against members of the Rohingya group, a distinct ethnic, racial and religious group that resides primarily in Myanmar's Rakhine State. These acts, which include killing, causing serious bodily and mental harm, inflicting conditions that are calculated to bring about physical destruction, imposing measures to prevent births, and forcible transfers, are genocidal in character because they are intended to destroy the Rohingya group in whole or in part. They have been perpetrated in manifest violation of the 1948 Convention on the Prevention and Punishment of the Crime of Genocide (the "Genocide Convention").[1] These acts are all attributable to Myanmar, which is thus responsible for committing genocide. Myanmar has also violated other fundamental obligations under the Genocide Convention, including by attempting to commit genocide; conspiring to commit genocide; inciting genocide; complicity in genocide; and failing to prevent and punish genocide.

3. In preparing this Application, The Gambia has taken care to pay close attention to the provisions of the Genocide Convention, including the circumstances of its adoption and its interpretation and application in the years following its entry into force on 12 January 1951. In

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar)

Cases Previous

LATEST DEVELOPMENTS

Press release 2020/14

26 May 2020

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar) - Extension of the time-limits for the filing of the initial pleadings

Available in:

English French

Order of 18 May 2020

Extension of time-limits: Memorial and Counter-Memorial

Available in:

English French

Press release 2020/4

28 January 2020

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar) - Fixing of time-limits for the filing of the initial pleadings

Available in:

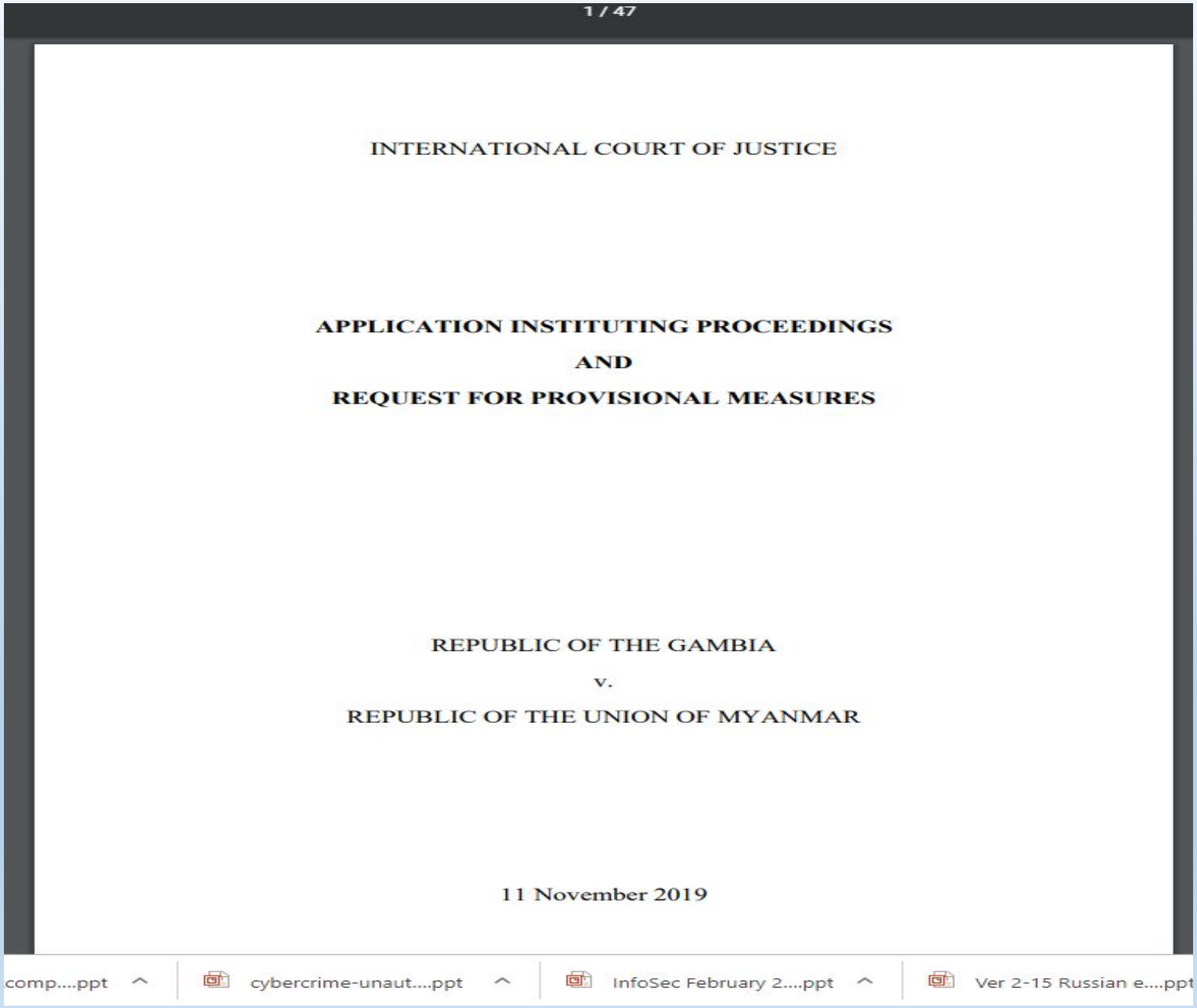
Overview of the case
Institution of proceedings
Provisional measures
Oral proceedings
Orders
Summaries of Judgments and Orders
Press releases

See multimedia galleries

See other cases involving
Gambia
Myanmar

See other cases involving
Provisional measures

https://www.icj-cij.org/files/case-related/178/178-20191111-APP-01-00-EN.pdf



APPLICATION INSTITUTING PROCEEDINGS AND
REQUEST FOR PROVISIONAL MEASURES

To the Registrar of the International Court of Justice,

The undersigned, being duly authorized by the Government of the Republic of The Gambia, states as follows:

1. In accordance with Articles 36(1) and 40 of the Statute of the Court and Article 38 of the Rules of Court, I have the honour to submit this Application instituting proceedings in the name of the Republic of The Gambia ("The Gambia") against the Republic of the Union of Myanmar ("Myanmar"). Pursuant to Article 41 of the Statute, the Application includes a request that the Court indicate provisional measures to protect the rights invoked herein from imminent and irreparable loss.

I. Introduction

2. This Application concerns acts adopted, taken and condoned by the Government of Myanmar against members of the Rohingya group, a distinct ethnic, racial and religious group that resides primarily in Myanmar's Rakhine State. These acts, which include killing, causing serious bodily and mental harm, inflicting conditions that are calculated to bring about physical destruction, imposing measures to prevent births, and forcible transfers, are genocidal in character because they are intended to destroy the Rohingya group in whole or in part. They have been perpetrated in manifest violation of the 1948 Convention on the Prevention and Punishment of the Crime of Genocide (the "Genocide Convention").[1] These acts are all attributable to Myanmar, which is thus responsible for committing genocide. Myanmar has also violated other fundamental obligations under the Genocide Convention, including by attempting to commit genocide; conspiring to commit genocide; inciting genocide; complicity in genocide; and failing to prevent and punish genocide.

3. In preparing this Application, The Gambia has taken care to pay close attention to the provisions of the Genocide Convention, including the circumstances of its adoption and its interpretation and application in the years following its entry into force on 12 January 1951. In

[1] Convention on the Prevention and Punishment of the Crime of Genocide (adopted 9 December 1948, entered into force 12 January 1951), 78 UNTS 277 [hereinafter Genocide Convention].

Our Focus- Actions of Individuals

•

The Regime

- crimes within the jurisdiction of an international court or tribunal
  - core crimes-*genocide, crimes against humanity, war crimes and aggression*
  - parallel crimes-piracy, slavery, *torture, terrorism,* drug trafficking and other offenses subject to international treaty
  - This regime includes
    - Substantive criminal law and
    - Procedural criminal law – the rules and process for investigation, prosecution and adjudication
    - Jurisdiction – both international and national tribunals may exercise power to adjudicate

Related Concepts

- Transnational Crime
  - Transborder impact or action-"transnational criminal law“
- International Criminal Law as protection for the Values of the International Order
  - Which would be?
- State Misconduct
  - But status as a state actor should not matter
- Crimes under International Law
  - consider the Nuremberg International Military Tribunal:
    - crimes against international law are committed by men, not abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced… Individuals have international duties which transcend the national obligations of obedience imposed by the individual state. Nuremberg IMT: Judgment and Sentences (1947) 41 AJ IL 172, 221

Sources of International Criminal Law

- TREATIES
  - 1949 Geneva Conventions, 1948 Genocide Convention, the statute of the International Criminal Court, Security Council resolution 827 (1993), International Criminal Tribunal for the former Yugoslavia, Security Counsel Resolution 955 (1994) International Criminal Tribunal for Rwanda per Article 25 of the UN Charter
  - Mandates for State domestic criminalization may not apply as matters of international law
  - Jurisdiction may depend on actions occurring within the territory of a signatory state
  - Treaty provisions may also be declaratory of customary law

`

- Customary International Law
  - Where statutes do not regulate, customary international law may be applied

- General Principles of Law
  - And the application of prior decisions, albeit non-binding
  - Some times there is resort to domestic law and treatises

International Criminal Law and Other Areas of Law

- Interplay with Human Rights Law
  - Impact of the Nuremburg IMT on later legal evolution of State violations of Human Rights
  - But HRL does not equal ICL, though overlapping
    - HRL procedures inform ICL prosecutions
    - But not all HRL violations are violations of ICL

A Body of Criminal Law

- International Law *and* Criminal Law
  - Nullum Crimen Sine Lege
    - Non-retroactivity and Notice – See Nuremburg and Tokyo IMT prosecutions
    - May resort to customary international law in compliance
  - Nulla Poena Sine Lege
    - Really, no crime without a defined punishment

The International Criminal Court

- Its Philosophy – Natural Law v. Positivism
  - Contra critical legal studies, gender studies, third world studies
- A Philosophy of a Criminal Law Regime?
- A Separate Philosophy of International Criminal Law?

- CRIMES within the jurisdiction of the ICC
  - genocide
  - crimes against humanity
  - war crimes
  - aggression
  - Article 5 ICC statute
- see subsidiary instrument-Elements of Crimes for greater definition of elements of the offenses
- see subsidiary instrument-Rules of Procedure and Evidence

- Article 21, sources of law-ICC Statute, subsidiary instruments, relevant treaties, rules of international law and "general principles of law"

The Aims, Objectives and Justifications of International Criminal Law

- Why are we here?

- The coercion of criminal jurisdiction
- What is the justification?
- What is the purpose?

International Society is not Domestic Society

- Mass criminality v. individual/small group
  - Individual v. group responsibility
- Purposes & Outcomes:
  - Reconciliation
  - Rule of Law
  - Domestic application
- Might ICJ be, at times, incoherent?
  - But true for any rule of law?

For What is International Criminal Justice

- Two approaches
  - Forward-looking – punishment to deter-deterrence
  - Backward-looking – punishment for accountability-retribution
    - The traditional approach to the purposes of sentencing

- Be cautious of over-expectations
  - Some from optimism
  - Some from exaggeration
  - Some from failures
- Mr. Justice Jackson on De facto impunity: “to mock the dead and make cynics of the living”

Retribution v. Deterrence

- Retribution must be proportionate
  - But how to make proportionate in a monstrous world?
    - And is it just victor's justice?

- Deterrence – the *Nikolic* Appeal:
  - All in armed conflict must be aware of obligations to other combatants and civilians
  - Develop a culture of respect for the rule of law, not simply fear
  - Deterrence must not be given undue prominence as to objectify the defendants in pursuit of goals

Incapacitation & Rehabilitation

- Utilitarian – prevention of future harm
- Reformation of the offender

Social Statement: Denunciation/Education

- “This IS WRONG!!!”
- Affirms correct values while condemning bad values
- Criticism: they are criminals, why would they care?
- Response: we need to build a normative system of values in this space

Vindicating the Rights of Victims

Recording History

- Setting out the truth so, perhaps, we don't do it again (or deny it happened!)
  - See, e.g., contemporary Holocaust denial
  - See, e.g, denial of Armenian genocide
  - See, e.g., denial of Rwandan genocide
    - ICTY *Krstic* judgment – intended to counter denial of Srebrenica massacre
- Criticism: trials not the place to write history

Critiques of Criminal Accountability

- Expensive
- Removed from the scene of the crime(s) (*locus delicti*)
- Is criminal law the right mechanism for large-scale international crimes
  - See, e.g. Arendt, Eichmann in Jerusalem?
  - Koskenniemi “punishing an individual does not come close to measure up to the [horror]”
- System Criminality: individual and collective responsibility
- Are ICJ trials designed only to justify those that created them?

Other Critiques

- Is it selective prosecution? If so, what does that tell miscreants?
  - Are only weaker, less developed countries targeted?
  - Should nations and their domestic laws be applied?
- Is it just *the arrogant imposition of Western values*?
  - Is disapproval of genocide, crimes against humanity and war crimes merely a cultural construct?
  - Does international customary law over-emphasize the law of dominant Western nations, especially in the ad hoc Tribunals?
- ***Nota Bene***: Rwanda, Uganda and the Democratic Republic of Congo have all asked for international prosecutions of international crimes.
  - Why?
  - Why not?

But in Sum…

- National and International Approaches can work together
- Impunity Not: should work towards a non-selective approach
- Is Some Enforcement Better than No Enforcement at All?
  - And does that then begin to limit the discretion of powerful States to
    - Commit misconduct
    - Ignore their misconduct
    - Fail to punish their own?
- Because what else might we have for the future?
  - You future, our future, everyone's future

So, changing a bit…

Consider how to…

- identify benefits of computing systems and resources within technologies
  -
  -
  -
- Identify risks of these technologies and allocate responsibility for the use and misuse of computing and ICT
  - ✔
  - ✔
- apply techniques to protect the rights and the benefits of computing and ICT within technologies
  - ❖
  - ❖
  - ❖

Artificial Intelligence and Human Rights

- The use of analytics in policing and public security offer exceptional benefits.
- But data modelling and statistical inference challenges social and legal bounds of privacy, personal autonomy and personal security.
  - Particularly when the analytical inferences go wrong or
  - Are wrongly used.
- As a result, these suggest a variety of liabilities-
  - administrative, legal and political
  - For what the future may hold

Consider…

- FBI Bulletin
  - 8-8-2019
  - Cmdr. Robert Davidson
    - Ventura County Sheriff
- The Future
  - The Good
  - The Bad
- But see
  - Ashley S. Deeks
  - Predicting Enemies
  - 104 Va. L. Rev. 1530
    - Dec. 2018

ARTICLES

Featured Articles | Legal Digest | Perspective | Focus | Additional Articles

August 8, 2019

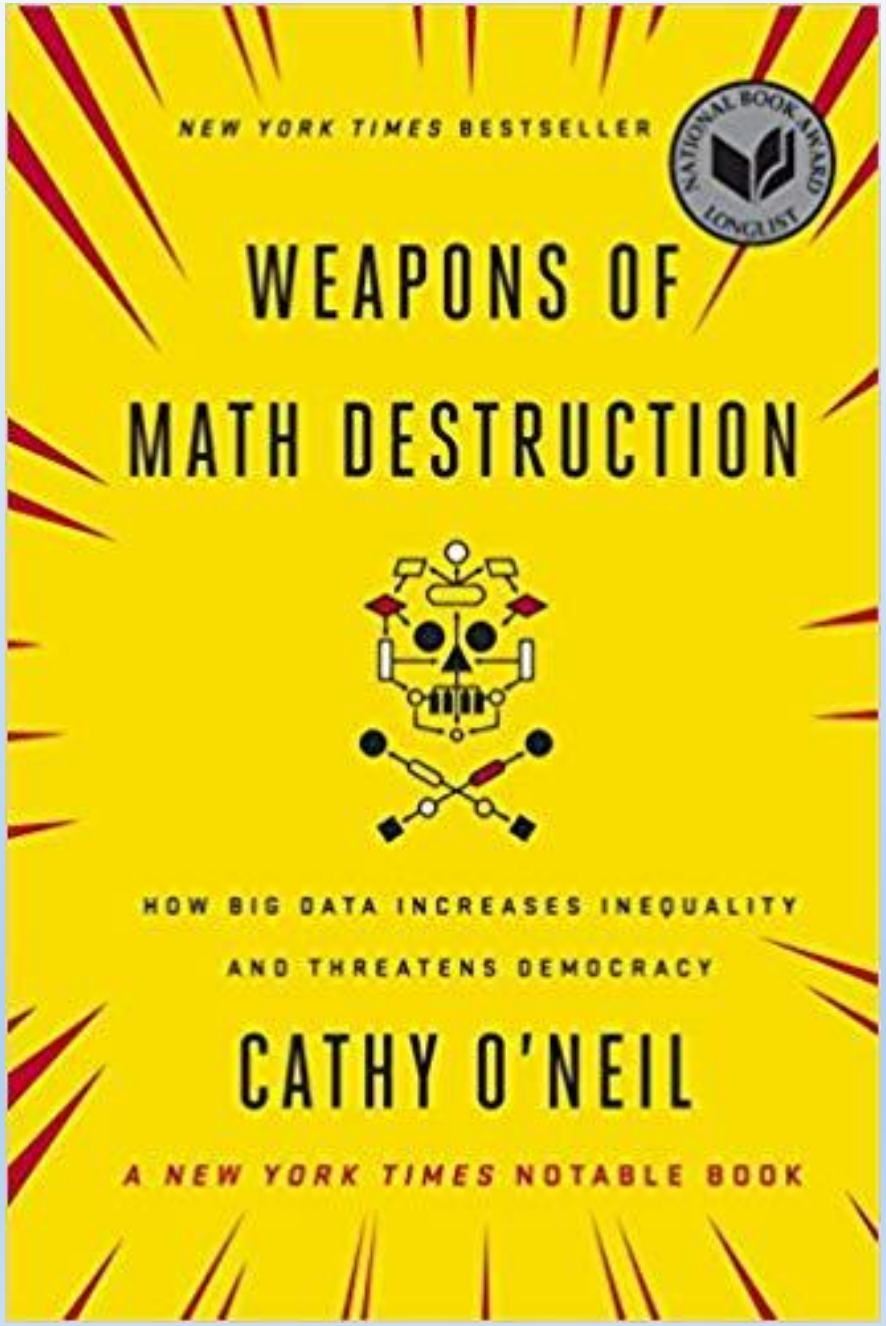
Twitter Facebook Email Print

Automated Threat Detection and the Future of Policing

By Robert Davidson, M.A.

Or

.


NEW YORK TIMES BESTSELLER
NATIONAL BOOK AWARD LONGLIST
WEAPONS OF MATH DESTRUCTION
HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY
CATHY O'NEIL
A NEW YORK TIMES NOTABLE BOOK

What will it be?

- 

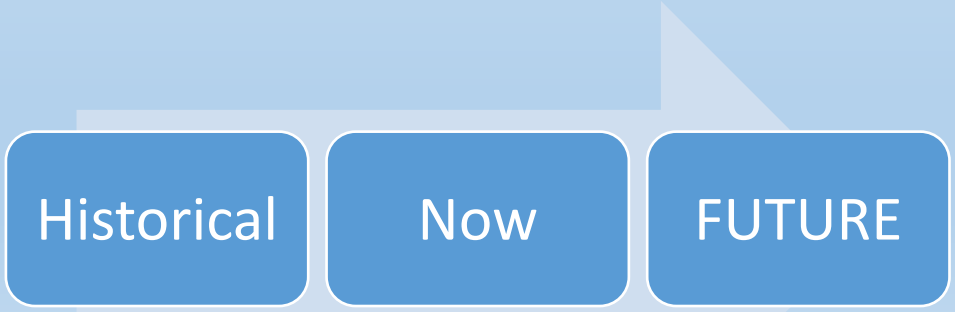
Or

.

Consider

- We examine this with US law and interrelationships with transnational legal developments
- a *Socio-Technical* System for Governance
  - Human decisions
  - Machine decisions
  - Responsibility?

- Analytics and computing become ubiquitous in data sources and uses, such as
  - The Internet of Things
  - The Smart City
  - Analytics for everything from toll use to bread and butter
  - evolving standards, e.g. the National Spatial Data Infrastructure, GDPR (EU)



Meta-Assumptions

- Our computational systems will be error free,
- Our computational systems will be human mediated as to correct any errors,
- Our computational systems will be too complex for the lawyers to figure out how to sue us.

Liability in Data Collection, Use and Disclosure

- Tort Liability/Products Liability
  - Mens rea
- Infringement of Civil Rights/statutory liability
  - Mens rea
- Criminal Liability
  - Mens rea

- Data
  - Collection, storage & transmission
- Analytics
  - Algorithms
  - Rendition
  - Visualization, Intel, Warrants
- Systems & Users

42 USC §1983

- Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia,
- subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof
- to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws,
- shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress,

18 USC § 242

- Whoever, under color of any law, statute, ordinance, regulation, or custom, willfully subjects any person in any State, Territory, Commonwealth, Possession, or District to the deprivation of any rights, privileges, or immunities secured or protected by the Constitution or laws of the United States, or to different punishments, pains, or penalties, on account of such person being an alien, or by reason of his color, or race, than are prescribed for the punishment of citizens,
  - shall be fined under this title or imprisoned not more than one year, or both;
- and if bodily injury results from the acts committed in violation of this section or if such acts include the use, attempted use, or threatened use of a dangerous weapon, explosives, or fire,
  - shall be fined under this title or imprisoned not more than ten years, or both;
- and if death results from the acts committed in violation of this section or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill,
  - shall be fined under this title, or imprisoned for any term of years or for life, or both, or may be sentenced to death.

Analytics Injury to Life & Person

- Life and Person
  - Loss of life, physical/mental injury to person
- Liberty and personal autonomy
  - Privacy rights and control of personal information
  - Reputation and public image
  - Freedom of action and person
- Property
  - Rights and interests
  - Informational
  - Costs of remediation and recovery

- Possible Vectors –
  -
  -
  -

Particular Federal Constitutional Concerns

- Fourth Amendment-secure from unreasonable searches and seizures
- Fifth Amendment-no deprivation of property or liberty without due process of law
- 14th Amendment-equal protection of the laws and due process of law

So, what possible injuries from flawed AI and predictive analytics?

-
-
-
-
-
-
-
-

A quick note on Ethics for Data Engineers

Challenger- when?

- January 28, 1986
  - Challenger launch
- January 27, 1986
  - Flight status meeting
- July 31, 1985
  - http://www.onlineethics.org/moral/boisjoly/MTImemo1.html

Interoffice Memo

31 July 1985

2870:FY86:073

TO: R. K. Lund

Vice President, Engineering

CC: B. C. Brinton, A. J. McDonald,

L. H. Sayer, J. R. Kapp

FROM: R. M. Boisjoly

Applied Mechanics - Ext. 3525

SUBJECT: SRM O-Ring Erosion/Potential Failure Criticality

Part II Here Comes The Judge!

- How do you really feel about a robotic system of justice?
- How about Robo-adjudication?
- Should we put ourselves out of a job?

Btw- Maneuvering Characteristics Augmentation System

Harbingers of the Future…

Cahoo, et al. v. SAS Analytics Inc., et al. ___ F.3d ___ (6th Cir. 2019) (US)

- Michigan residents were, **based on data analytics**, erroneously found to have committed unemployment benefits fraud and denied benefits,
  - leading to eviction, bankruptcy and wrongful seizure of tax refunds.
- State agency employees were sued for deprivation of civil rights pursuant to 42 USC section 1983
  - for the implementation and oversight of the automated computer system that falsely determined the plaintiffs had committed fraud.
- The agency defendants sought qualified immunity for their actions
  - for denial of equal protection, illegal seizure and denial of due process.
- *OUTCOME?*

Legal Standard

- Qualified Immunity –
  - “First, taken in the light most favorable to the party asserting the injury, do the facts alleged show that the officer’s conduct violated a constitutional right?
    - damage claims against government officials arising from alleged violations of constitutional rights must allege, with particularity, facts that demonstrate what *each* defendant did to violate the asserted constitutional right.
  - Second, is the right clearly established?” (…if ‘[t]he contours of the right [are] sufficiently clear that a reasonable official would understand that what he is doing violates that right.’”)
    - Plaintiff bears burden of proving no qualified immunity;

Human Rights (Constitutional) Violations -Due Process of Law, Equal Protection, Unlawful Seizure

- The Fourteenth Amendment provides that no state shall "deprive any person of life, liberty, or property, without due process of law." U.S. Const. amend. XIV, § 1.
  - "[T]he Due Process Clause provides that certain substantive rights—life, liberty, and property—cannot be deprived except pursuant to constitutionally adequate procedures."
    - …"[T]he Supreme Court has held that the hallmark of due process is that a deprivation of a property interest must be 'preceded by notice and opportunity for hearing appropriate to the nature of the case.'"
- Equal Protection 14th Amendment - safeguards against the disparate treatment of similarly situated individuals as a result of government action that 'either burdens a fundamental right, targets a suspect class, or has no rational basis.'"
- The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated . . . ."

The case on appeal

- Government officials Julie, Steven, Shemin, Dorris ,Debra ,and Sharon appeal the district court's decision denying their Motion to Dismiss on qualified immunity,
  - in this 42 U.S.C. § 1983 action alleging that the Individual Agency Defendants implemented and oversaw an automated computer system that falsely determined that Plaintiffs had committed unemployment insurance fraud and
  - deprived Plaintiffs of protected property interests as a result of those erroneous fraud determinations, without providing Plaintiffs with adequate pre-deprivation notice, in violation of the Fourth and Fourteenth Amendments.

chronology

- **October 2013,** Michigan's Unemployment Insurance Agency ("Agency") began administering Michigan's unemployment benefits system through an automated program called MiDAS.
  - The Agency designed, created, and implemented MiDAS to render automated determinations of fraudulent conduct.
- MiDAS searched for discrepancies in the records of individuals who were receiving—or who, in the six years prior to the program's introduction, had received—unemployment insurance benefits.
  - The Agency had access to claimant records from employers, state agencies, and the federal government;
  - it coordinated with those entities and "cross-checked" information about claimants that could affect their eligibility for benefits.

- When MiDAS detected unreported income or “flagged” other information about a claimant, it initiated an automated process to determine whether the individual had engaged in fraudulent behavior. (*Id*. at ¶51.)
  - MiDAS flagged claimants if it detected any discrepancy between information submitted by a claimant when applying for benefits and a record submitted by an employer.
    - MiDAS did not investigate whether these discrepancies resulted from employer error or were the product of a good-faith dispute.
  - MiDAS also flagged claimants through an “income spreading” formula;
    - MiDAS calculated a claimant’s income in a fiscal quarter and averaged the claimant’s weekly earnings, even if the claimant did not actually make any money in a given week. (*Id*. at PageID #751, ¶8.)
    - If the employee reported no income for any week during a quarter in which he or she earned income, MiDAS automatically determined that the claimant had engaged in fraud.
  - The Agency made no effort to assess whether the claimant truthfully reported no income for the week(s) in question.

- When a claimant was “flagged” for possible fraud,
  - MiDAS did not inform the claimant about the basis for the Agency’s suspicion or provide the claimant with any information to allow him or her to rebut the fraud charge.
- MiDAS did not allow for a fact-based adjudication or give the claimant the opportunity to present evidence to prove that he or she did not engage in disqualifying conduct.
- Instead, Midas automatically sent claimants multiple-choice questionnaires.
- Claimants were told they had ten days to respond to the potential disqualification by answering the following questions:

MIDAS robo-questionaires

- Did you intentionally provide false information to obtain benefits you were not entitle[d] to receive?
- Yes No
- Why did you believe you were entitled to benefits?
  - 1. I needed the money
  - 2. I had not received payment when I reported for benefits
  - 3. I reported the net dollar amount instead of the gross dollar amount paid
  - 4. I did not understand how to report my earnings or separation reason
  - 5. I thought my employer reported my earnings for me
  - 6. Someone else certified (reported) for me
  - 7. Someone else filed my claim for me
  - 8. Other

- The questionnaires did not provide the claimants with any information about why the Agency suspected they had engaged in fraud.

- If a claimant answered any of the questions
- in the affirmative, or
- failed to respond to the questionnaire in ten calendar days,
- "MiDAS robo-adjudicated the fraud issue and automatically determined that the claimant knowingly and intentionally misrepresented or concealed information to unlawfully receive benefits."
  - From October 2013 to August 2015, MiDAS exclusively determined whether claimants engaged in fraud—no human being took part in this process.

Further…

- MiDAS sent the questionnaires to claimants' accounts established online on the Michigan Web Account Management System.
- But many claimants' accounts were dormant; MiDAS reviewed unemployment benefits claims starting six years before MiDAS became operational,
  - and many claimants did not have a reason to check their accounts.
- And MiDAS did not take any additional steps—
  - such as sending emails,
  - regular mail, or
  - making phone calls—
- to notify claimants that the questionnaire had been sent.

- When MiDAS determined that a claimant committed fraud, the individual's right to benefits terminated immediately.

- In addition, claimants were automatically assessed severe monetary penalties:
  - restitution and a penalty for fraudulent misrepresentation equal to four-times the amount of unemployment benefits received (or sought)—the maximum penalty permitted under state law.

- The Agency assessed the penalties even when claimants did not actually receive benefits.
  - Many claimants were assessed penalties that ranged from $10,000 to $50,000.
    - Some received penalties greater than $187,000.

- After MiDAS determined that a claimant had committed fraud, the Agency automatically sent the claimant a statement letter.
- The letter demanded that the claimant repay benefits, penalties, and interest.
- The letter provided that “penalties for non-payment may include
  - interception of the claimant’s state income tax refund,
  - interception of the claimant’s federal income tax refund,
  - garnishment of wages, and
  - legal collection activity through a court of law.”

- The Agency often
- failed to send the letters, or
- sent them to the wrong address,
- because the Agency did not make any effort to verify that the statements were sent to the claimant’s current address.

- The Agency also sent claimants a second form letter, titled a “Notice of Determination.”
- This letter stated, “Your actions indicate you intentionally misled and/or concealed information to obtain benefits you were not entitled to receive.”
- But the Notice of Determination letter did not inform claimants about the factual basis for the fraud determinations.
- The Notice of Determination letter also included a document titled “Restitution (List of Overpayment),” which contained the overpayment amount and demanded repayment of the benefits allegedly received and the statutory penalty.

- The only time real-life Agency employees evaluated a particular instance of suspected fraud was when a claimant filed an appeal.
- Claimants had 30 days to appeal the fraud determination to an Administrative Law Judge ("ALJ").
- But "the vast majority" of claimants did not know about the fraud determination until the window to appeal had expired and they had been assessed thousands of dollars in fines.
- And when claimants attempted to appeal,
  - Agency employees informed them that they could not appeal because more than 30 days had passed, even if the claimants still had the right to appeal because they never received notice.
- According to the Michigan Auditor General, the Agency never answered over 90% of the calls to its "Help Line."
  - of the last 50,000 calls the "Help Line" received before the Auditor General conducted the audit, "not a single one had been answered or returned."

The Human Touch-*not*

- the Agency made no attempt to consider the facts or circumstances of a particular case, or
  - determine whether the alleged fraud was intentional, negligent, or simply accidental.
- Further, this system was deeply flawed; the Michigan Auditor General
  - reviewed over 22,000 of MiDAS' fraud determinations and
  - found that 93% of them did not actually involve fraud.
- **In other words, 93% of MiDAS' fraud adjudications were false-positives.**
- Even after the Auditor General made its findings, the Agency continued to use MiDAS to attempt to detect fraud.
  - While humans had some involvement, the process was still based around MiDAS' faulty algorithms. And Plaintiffs allege even with human involvement, approximately 50% of the fraud determinations were invalid.

Injuries to plaintiffs

- Patti Jo – false determination, denied benefits, evicted
- Kristen – false determination in 2016 of 2010 benefits, forced into bankruptcy
- Khadija – false determination saying owed $26,000
- Michelle-false determination, state and federal tax refunds seized 2015-16 (learned of determination only from IRS seizure letter)
- Hyon – false determination, state and federal refunds seized 2012-14 (learned of determination only from IRS seizure letter)

- The Agency Defendants knew that there were “serious problem[s]” with MiDAS and that “the vast majority” of fraud determinations were invalid.

- These problems were “widely-known” throughout the Agency.

- Despite knowing of the high error rate and high percentage of erroneous fraud determinations, they “changed nothing and forged ahead” with MiDAS.

- G “ordered state attorneys general . . . to conduct business as usual” and to “continue to contest claimants’ protests and appeals and [to] continue with collection activities” even though he knew the fraud determinations were false.
- M “instructed various attorneys general to continue to oppose claimants’ attempts to discharge fraud-based debt in bankruptcy proceedings by filing adversary proceedings, even when it was obvious that the underlying judgment . . . was based on an invalid fraud determination.”
- S “continued to direct subordinates to pursue aggressive collection activities . . . includ[ing] tax refund intercepts and wage garnishments” even though he knew the “vast majority” of fraud adjudications were invalid.
- B “ continued to instruct her subordinates, including the claims examiners, to pursue invalid fraud charges.”
- MM “continued to pursue the same defective” policies despite knowing about MiDAS’ problems and invalid fraud determinations.
- “<u>when certain ALJs expressed concerns about the Agency’s practices” due to the high rates of invalid fraud determinations, M removed them from hearing fraud cases.</u>

Held

- The Court holds that qualified immunity does not protect the Individual Agency Defendants from Plaintiffs' due process claim because Plaintiffs plausibly alleged that the Individual Agency Defendants violated Plaintiffs' clearly-established due process rights.
  - qualified immunity protects the Individual Agency Defendants from Plaintiffs' equal protection claim because Plaintiffs failed to allege a plausible equal protection violation.
  - qualified immunity protects the Individual Agency Defendants from Plaintiffs' Fourth Amendment claim because Plaintiffs failed to plausibly allege that the Individual Agency Defendants violated Plaintiffs' clearly-established Fourth Amendment rights.

Thoughts?

The Los Angeles Police Department and its data-driven programs

- The Los Angeles Police Department uses data to pinpoint crime “hotspots” and violent offenders using its databases and various algorithms.
  - But these have been challenged as having inherent biases based on race, leading to the end of one such program.
- Further, certain of these data tools have been challenged as lacking empirical validation of the accuracy of the systems;
  - one challenge tool was designed to protect where crimes would likely occur in the next.
- The inspector General for the Los Angeles Police Department conducted an audit of the use of data programs finding, inter alia, that officers “… Used inconsistent criteria to identify people with criminal histories…”
  - The Department has suspended use of one tool and its tracking database in August, 2018

Report of the Inspector General-LAPD
REVIEW OF SELECTED LOS ANGELES POLICE DEPARTMENT DATA-DRIVEN POLICING STRATEGIES
March, 2019

- Review of the LASER Program
- Review of PREDPOL
- Review of ELUCD
- Retention, sharing and reporting of data
- Recommendations

Los Angeles Strategic Extraction and Restoration (LASER) Program

- contains both a person-based and a location-based component;
  - Palantir generated chronic offender bulletin, but with disclaimer
- LASER has five primary objectives in furtherance of the overall goal:

  Extract offenders from specific neighborhoods in the areas.

  Restore peace to neighborhoods and communities.

  Remove the anonymity of gun offenders.

  Remove the anonymity of gang members.

  Reduce gun and gang-related crime.
- Chronic Offer Program and LASER Zones hotspot identification

Chronic Offender Program

- was initially to identify persons who were committing violent crimes in a target area and to remove them from the area, presumably by arresting them.
- The point system used for the Chronic Offender Program has changed somewhat since it was first implemented. At the inception of the program, each person who was the subject of a work-up received the following:
  - • 5 points if the individual is a gang member.
  - • 5 points if the individual is on parole or probation.
  - • 5 points if the individual had any prior arrests with a handgun.
  - • 5 points if the individual had any violent crimes on his or her rap sheet.
  - • 1 point for every “quality police contact” in the last two years.8

- In 2017, two criteria in the point system above were modified to include the following considerations:
  - • Identify the number of violent crime arrests the individual had over the last two years. Apply 5 points for each violent crime arrest.
  - • Determine whether the individual has used a gun in the course of his/her activities. Apply 5 points for each incident involving a gun over the last two years.

And then…

- Once developed, an Area's list of 12 Chronic Offenders is presented to the Area Commanding Officer for approval. The Area Commanding Officer then determines which field personnel (Patrol Unit, Gang Enforcement Detail, Parole Compliance Unit, etc.) to assign to a given Chronic Offender for the purposes of conducting follow-up with that individual.
- Based on Department materials provided to the OIG, the Department's recommended follow-up activities included: 1) sending a letter to the offender; 2) conducting warrant checks; 3) conducting parole/probation compliance checks; and 4) conducting door knocks and advising the offender of available programs and services designed to reduce the risk of recidivism. Personnel who are assigned an offender are to provide a status update to their Commanding Officer every two weeks regarding what actions have been taken with that offender.

Location-Based Strategy: LASER Zones

- ArcMap and the Crime Analysis Mapping System (CAMS)
- After designation, field personnel assess potential causes of crime
- Interventions include abatement, eviction, licensing/conditional use permits, or changes in environmental design.
- Officers encouraged to spend time in designated zones for increased police visibility, keyed to the times when crimes tended to occur; this time is recorded.
- Evaluations of 2011-2012 data showed impact in the pilot area of Part One violent crimes declining but not in other designated areas.

Review

- Program materials
- Training
- Site visits
  - Inconsistent practices and use of tool
- Review of Chronic Offender Program Data
  - Inconsistencies
  - Inconsistent retention of generated bulletins
- Review of laser zone and anchor point data

PredPol, a predictive policing system that is location-based

- Past evaluations-in one study crime reduction of 7.4%, but in another no difference
- As with LASER, the OIG's review of PredPol dosage revealed potential discrepancies with how dosage data is being collected that made it difficult to draw conclusions about the effectiveness of the system in reducing vehicle or other crime.
- the OIG found that the impact of PredPol on the community seems to be limited by the fact that the majority of PredPol visits to a given location appeared to be very short and, in most cases, occur only a few times per month. The OIG did note some areas, however, that were subject to many visits or, in some cases, relatively long visits. The collection of more precise data – particularly data that is able to tie PredPol locations to the types of enforcement activities occurring there – would assist in determining the overall impact on the community.

The ELUCD survey platform, which is designed to inform police departments about public sentiment

- Survey push company the advertisements
- Each survey asks three main questions:
  - 1. Do you feel safe in your neighborhood?
  - 2. Do you trust the police?
  - 3. Are you confident in your police department?
- Talked with the company but would not release their data
- Without having access to ELUCD's datasets, the OIG did not examine this program further.

RETENTION, SHARING, AND REPORTING OF DATA

Recommendations

- **A. Offender-Based Programs**
- To the extent that the Department continues with any data-driven, offender-based policing strategies, the OIG recommends that it:
- 1. Establish formal written guidelines, to be approved by the BOPC, which:
- a. clearly articulate the goals and expected results of the program;
- b. provide clear direction of the selection process including: time parameters, procedures for conducting a work-up, and specific crimes the program is intended to target;
- c. avoid designating a required minimum number of people to be selected;
- d. provide disclosure and appeal processes for each person selected for the program;
- e. provide direction on how and when a person is to be removed from the program;
- f. clearly define any aspects of the strategy that may be adapted to meet the needs of individual Areas;
- g. include mandatory program activities (such as providing an offender a letter); and,
- h. specify prohibited program activities or limits (such as the frequency with which a person may be contacted)

- 2. Modify its Offender Database to capture:

- a. a description of why a person was selected for the program, and any specialized Department strategy related to that person, where relevant;
- b. the date a person is added to the database;
- c. the date a person becomes active or inactive;
- d. each person’s descent information for reporting purposes;
- e. detailed information about the nature and intent of any LASER-driven activity;

- f. results of any LASER-driven activity; and,
- g. the source of any status updates regarding a person in the database (e.g., a records search).

- 3. Specify a retention policy for any bulletins or related documents, and require that all Areas use a format that has been approved by the City Attorney's Office.

- 4. Ensure that any revisions to the language used in the Offender Bulletin or Offender Letter are approved by the City Attorney.

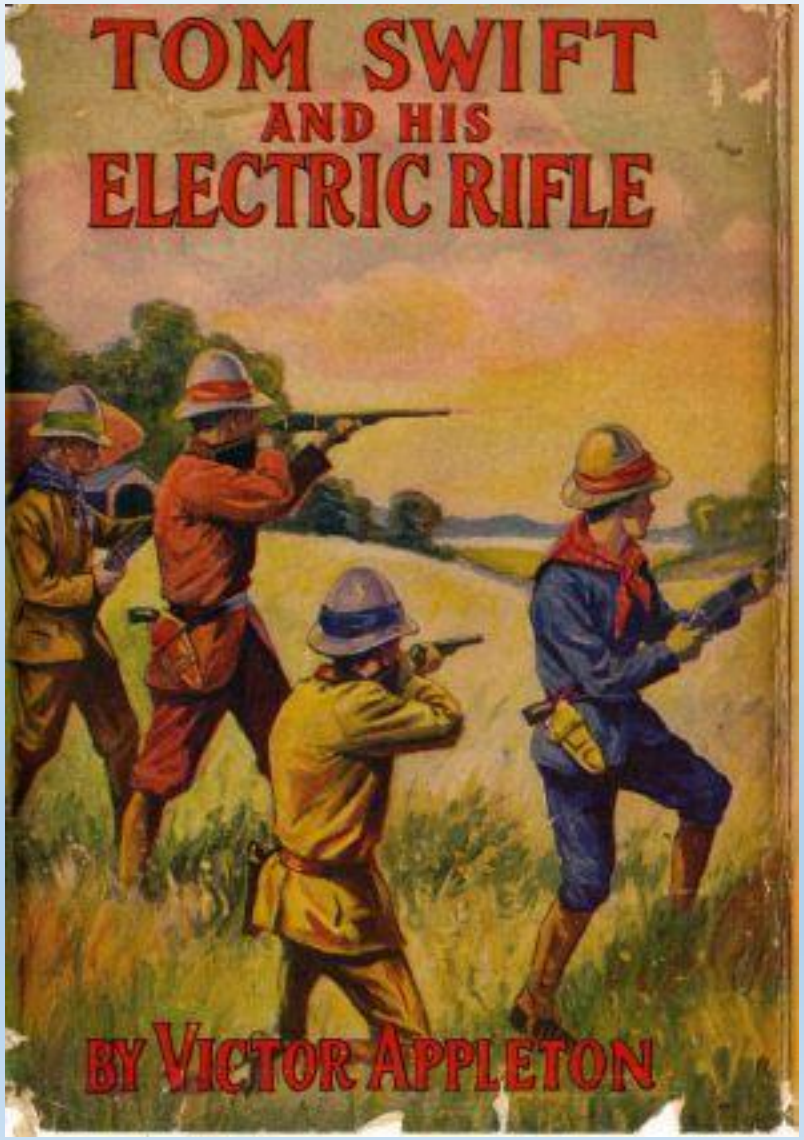
- 5. Develop a consistent training process to be completed prior to use of the program.

- 6. Develop an oversight and audit structure to ensure the consistency of the data, as well as the consistent utilization of the program. As part of this process, centralize the maintenance and oversight of the Offender Database.

- **B. Location-Based Programs**
- With respect to the location-based components of Operation LASER and PredPol, the OIG recommends that the Department:
- 1. Establish formal written guidelines that specify how Areas are to identify LASER Zones and Anchor Points, when to conduct assessments of the Zones, and what strategies and activities are to be taken at these locations.
- 2. Ensure that LASER Zones and PredPol locations do not encompass LAPD facilities.
- 3. Reconcile and address inconsistent data or discrepancies between Palantir and PredPol datasets to ensure that dosage amounts are captured accurately.

- **C. Reporting and Evaluation**
- The OIG also recommends that the Department:
- 1. Develop a system for regular reporting of basic usage and outcome data to the Commission and the public. Information to be tracked might include the types of data contained in this report, including dosage and crime data, general statistical information about the people and locations targeted for intervention, and information about activities and outcomes related to the Department's data-driven programs.
- 2. Look for opportunities to obtain independent evaluations of the efficacy and impact of each data-driven policing program.
- 3. Consider seeking community and Commission input prior to the implementation of any new data-driven policing strategies or any significant revisions to the current data-driven programs.

One Model for Anticipatory Analysis for Police Technology

- 

Axon Analysis of Facial Recognition Software

- Worked with more than 18,000 law enforcement agencies on LE technology of various types
- Asserts 48 to 79 major city LE agencies in North American are its customers
- Established ethics board to examine issues relating to AI and other policing technologies

First Report of the Axon AI & Policing Technology Ethics Board, *June, 2019*

- Board operations & Lessons Learned
- Product evaluation framework
- Early thoughts and recommendations regarding facial recognition technology
- Conclusion

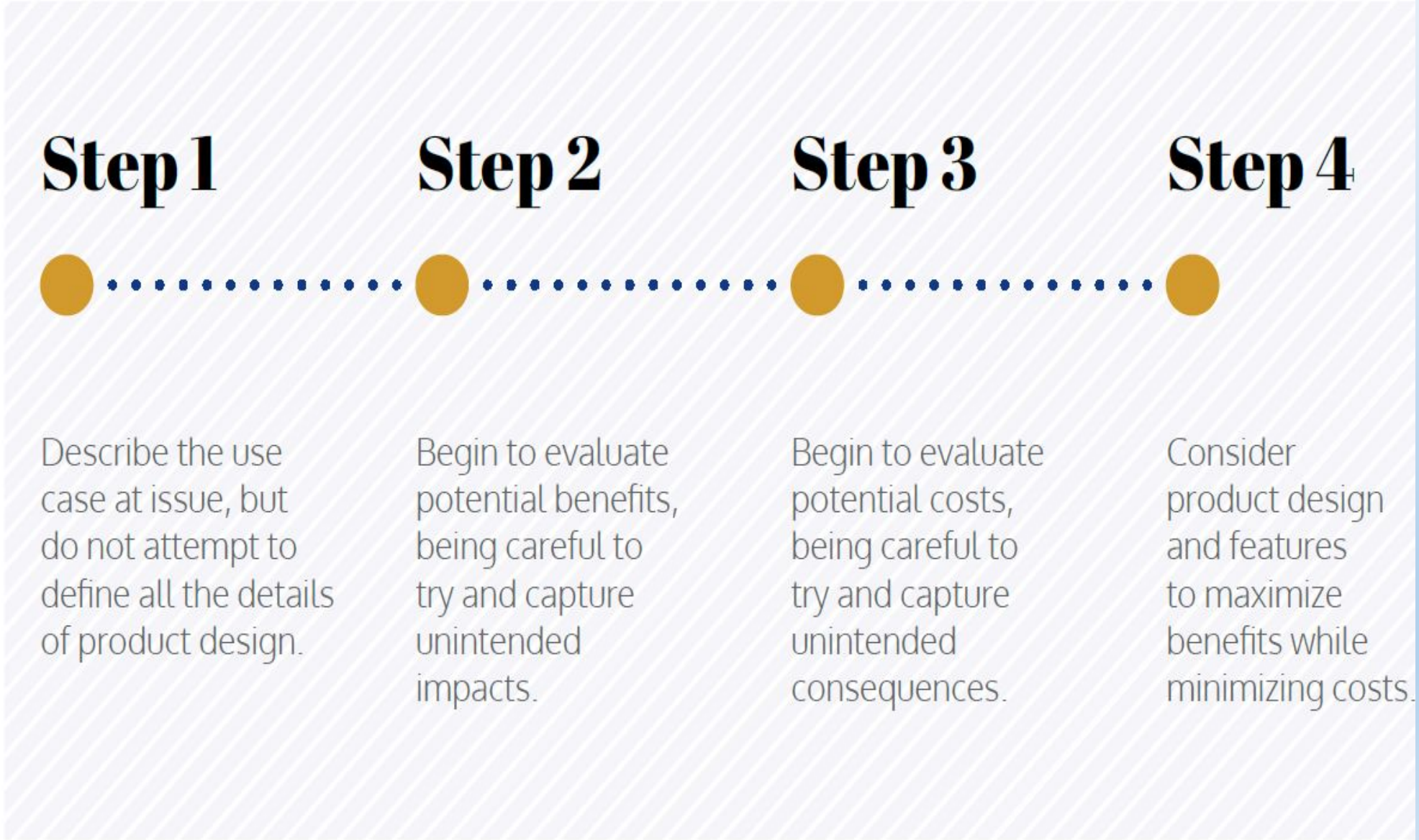
Board operations & Lessons Learned

- Diversity an issue-
  - Members of the civil liberties and racial justice community declined participation
  - See, open letter from the leadership conference on civil rights expressing interests and concerns
- Board given high degree of independence
- Unique opportunity to influence law enforcement technology broadly given the preeminence Of Axon
- Important to focus given the huge scope of this area, thus looking at AI-power technologies
- Required:
  - the free exchange of information, productive meetings, use of NDA's, establishment of operating principles, ombudsman/process for anonymous employee input, effective meeting facilitation, independent staff support (The Policing Project)
- Important:
  - Early Board Involvement; Iterative work process;, Public engagement and transparency

The Board is in Conversation with Axon About:

- Internal Trainings on Bias
- Creating Products Designed to Improve Policing Transparency and Democratic Accountability
- Devising Internal Protocols to Incorporate Ethical Frameworks for Assessing New Products
- Axon's Role and Responsibility for the Products It Produces
- Pivoting Axon's View of Its Customer Base from Law Enforcement to the Public

Product evaluation framework



Guidance on benefits assessment

- 1 what is the specific problem the products intended to solve
- 2 how important/what is the magnitude of the problem you expect to solve
- 3 how certain is it that the technology will address the problem
- 4 could using the technology have unintended or secondary benefits for:
  - Minimize criminalization of low-level offenses?
  - Additional control and protection of personal data?
  - Mitigation of racial and/or identity bias?
  - Improved transparency or public trust?
  - Better compliance with U.S. constitutional requirements?
  - Other societal benefits?

Guidance-assessing costs

1. Once deployed can the technology be used or misused in on anticipated ways?
2. Will it lead to greater criminalization or to policing in counterproductive ways?
3. Will the technology impact personal information privacy?
    1. What is the data captured, retained, owned, accessed, protected
4. Does the technology implicate potential biases, especially racial or other identity factors, whether in design or use?
5. Does the technology create transparency -related concerns with the public?
6. Does the technology risk, directly or indirectly, violations of constitutional or legal rights?
7. Are there other potential social costs that have not been considered, such as impact on specific groups, "mission creep", historical issues, industry influence, global human rights?

Early thoughts and recommendations regarding facial recognition technology

- Use of face recognition comes with serious concerns.
  - Face matching, face detection, face re-identification
    - Use in Axon's redaction assistant tool for body cam footage.
  - False positives and False negatives; quality of images
    - Disparities in accuracy with gender, age, race
  - Privacy; see, e.g., United States v. Jones, Sotomayor, J, concurring
  - Use by regimes globally
- Process to date-concerns with insufficient engagement among all stakeholders and rapid deployment without full consideration of all the issues

Axon Advisory Board Use Case Examples- Good v Bad

Use Case #1

Using face recognition during a motor vehicle stop to identify a driver who has forgotten her license.

Use Case #2

Using face recognition to identify missing persons (e.g., Silver Alerts[5] or Amber Alerts) who are voluntarily added to the system by family members.

Use Case #3

Using face recognition to identify a small subset of individuals designated to a "most wanted" list by local law enforcement.

Conclusion-1

- **Face recognition technology is not currently reliable enough to ethically justify its use on body-worn cameras.**
- **At the least, face recognition technology should not be deployed until the technology performs with far greater accuracy and performs equally well across races, ethnicities, genders, and other identity groups.**
- **Whether face recognition on body-worn cameras can ever be ethically justifiable is an issue the Board has begun to discuss**

Conclusion-2

- **When assessing face**
- **recognition algorithms,**
- **rather than talking about**
- **“accuracy,” we prefer to discuss**
- **false positive and false negative**
- **rates. Our tolerance for one or the**
- **other will depend on the use case.**

Conclusion-3

- **The Board is unwilling to**
- **endorse the development**
- **of face recognition technology of**
- **any sort that can be completely**
- **customized by the user. It strongly**
- **prefers a model in which the**
- **technologies that are made**
- **available are limited in what**
- **functions they can perform, so as**
- **to prevent misuse by customers.**

Conclusion-4

- **No jurisdiction should**
- **adopt face recognition**
- **technology without going through**
- **open, transparent, democratic**
- **processes, with adequate opportunity**
- **for genuinely representative**
- **public input and objection.**

Conclusion-5

- **Development of face**
- **recognition products should**
- **be premised on evidence-based**
- **benefits. Unless and until those**
- **benefits are clear, there is no**
- **need to discuss costs or adoption**
- **of any particular product.**

Conclusion-6

- **When assessing the costs and**
- **benefits of potential use cases,**
- **one must take into account both**
- **the realities of policing in America**
- **(and in other jurisdictions) and**
- **existing technological limitations.**

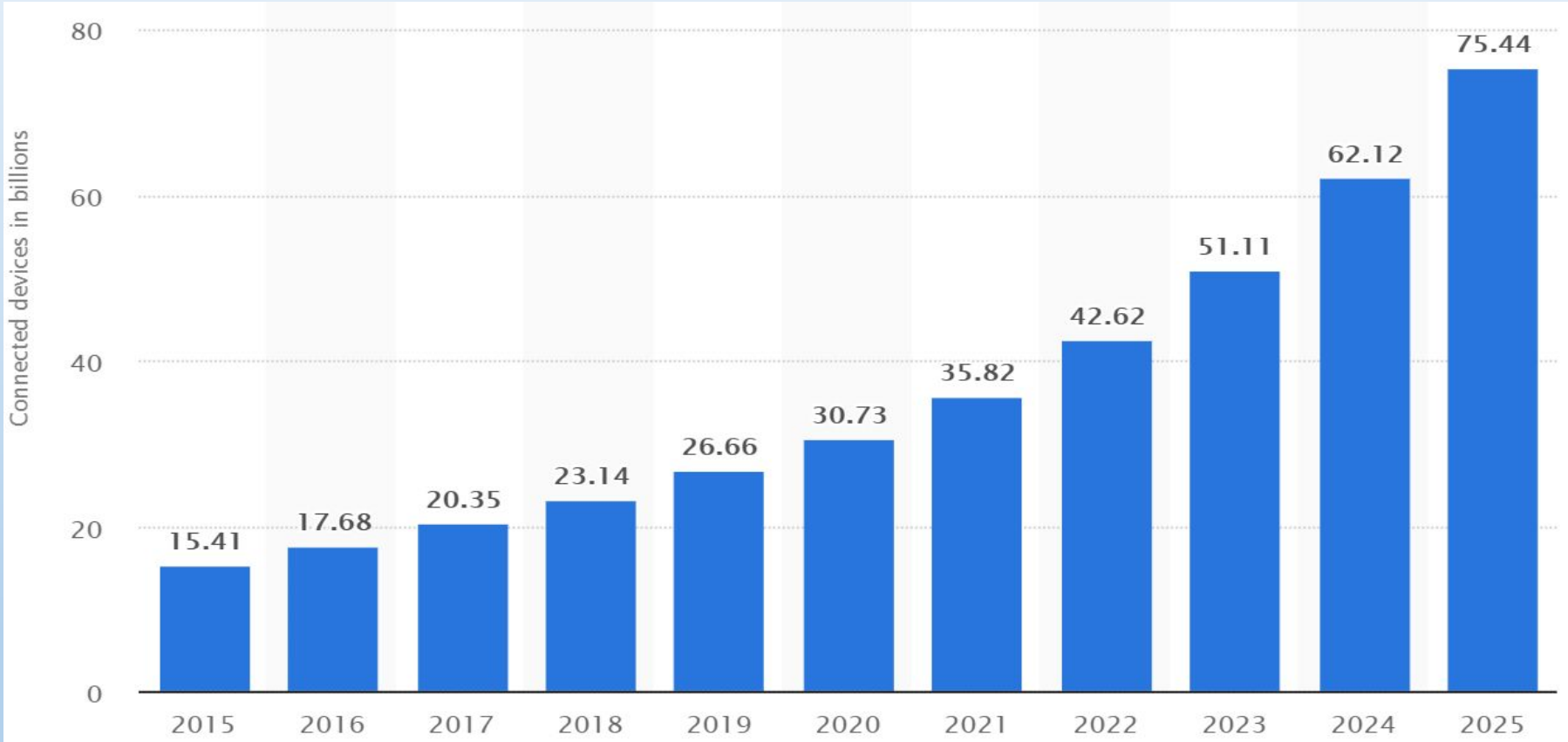
In Closing

- “This is the first report of our AI and Policing Technology Ethics
- Board. We intend to continue our work, along the lines that we
- have set out here, and to issue reports in the future if and when
- we believe we have things of value to say or simply to inform
- the public of our progress. We very much hope our thoughts
- here will influence Axon itself, which has convened us, as well
- as the broader technology industry, particularly those industry
- segments that make products available to governments.”

- The data-driven police analytics present significant challenges in law, ethics and public policy.
  - Such analytics and data-driven actions manifest all the challenges relating to the use of expert systems and information assurance, including authentication, validation and protection of this data.
  - And we have seen that the data generation, transmission and collection begin the parallel issue similarly seen in information security and assurance.
- With more modeling and analysis, the predictive ability for behavioral inferences has increased, posing different legal, administrative and political concerns.
- We must anticipate and address them to assure their benefits for public safety .

IOT, Ethics & Human Rights

The Internet of Every Thing



DESCRIPTION SOURCE

by Statista Research Department,
last edited Nov 27, 2016

The total installed base of Inte
connected devices is projected
billion worldwide by 2025, a fiv
years. The IoT, enabled by the
Internet technology, is the nex
delivering Internet's promise o
connected place.

What is the IoT?

One estimate:

- As of March, 2019 4.4 billions of the world's 7.7 billions are internet users
- Africa showing the strongest growth from around 2% in 2005 to 24% in 2018
- But,
  - ITU noted problems remain worldwide for women, girls, older people, indigenous populations and those in poor regions
  - So, why does this matter?

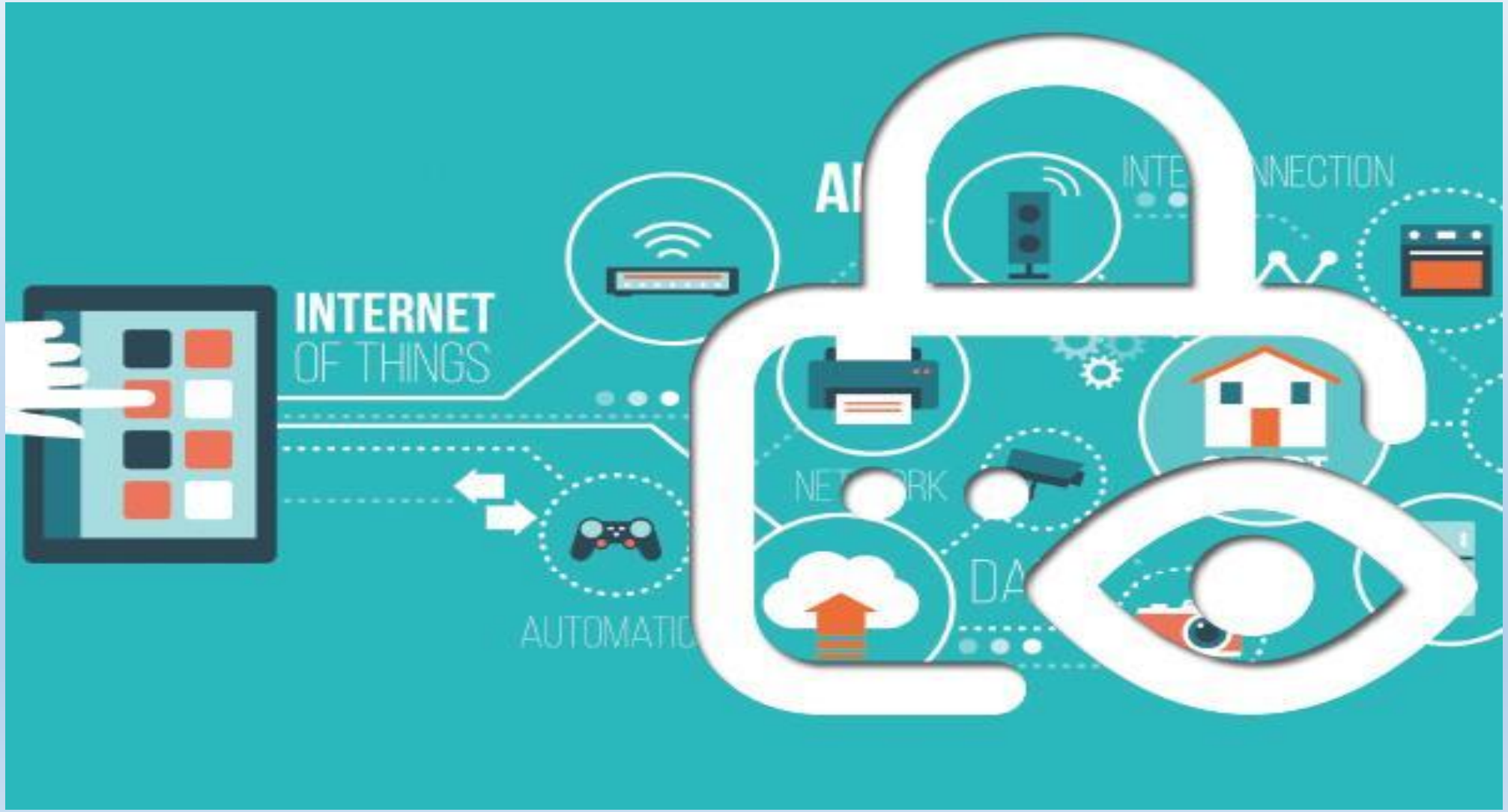
Irony Of The Modern Internet

- Yemini: "[it] provides more expressive capacity to individuals than ever before, also systematically diminishes their liberty to speak."
- His list of the destructive forces :
  - interference from multiple sources:
  - state-encouraged private interference;
  - multiple modes of interference;
  - new-media concentration;
  - lack of anonymity; and
  - lack of inviolability.

The Internet of Things… (courtesy of US NIST)

And as the Hong Kong Lawyer notes: **How Internet of Things May Expose Your Privacy**

http://www.hk-lawyer.org/content/how-internet-things-may-expose-your-privacy

- 

It is all about people

- It is about human dignity
- It is about human potential
- *It is still very much about people, their families and their communities!*

ICT & Ethics is Evolving:

The **Menlo Report:** Ethical Principles Guiding Information and Communication Technology Research August 3, 2012
https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf

- The Menlo Report…
- proposes a framework for ethical guidelines for
  - computer and
  - information security
  - research
- based on the principles set forth in the 1979 Belmont Report…
- …

Who has an interest or is effected?

- **Stakeholder Perspectives and Considerations**
  - **Researchers**
  - **Human Subjects, Non-subjects, ICT Users**
  - **Malicious Actors**
  - **Network/Platform Owners and Providers**
  - **Government/Law Enforcement**
  - **Government/Non-Law Enforcement (e.g., public services)**
  - **Society collectively**

Respect for Persons

- Respect for Persons
  - Personal autonomy
  - Protection of those with reduced autonomy (ill, handicapped, youth, inmates)
- Informed Consent
  - Activities, risks, benefits, choice
  - Waiver where minimal risk and needed for research

Beneficence

- maximization of benefits and minimization of harms
- **Identification of Potential Benefits and Harms**
- **Balancing Risks and Benefits**
- **Mitigation of Realized Harms**

Justice

- Fairness
- Equity

Respect for Law and Public Interest

- Compliance
  - identify laws, regulations, contracts, and other private agreements that appky to their research, and
  - design and implement ICTR that respects these restrictions.
- Transparency and Accountability
  - mechanism to assess and implement accountability
  - Responsibility for actions and outcomes

Implementing the Principles and Applications

- IRB oversight? (outside oversight)
- ICT *Researcher* awareness and use? (internal self-evaluation)
- ICTR application?

Menlo Report Companion :
Applying Ethical Principles to ICT Research

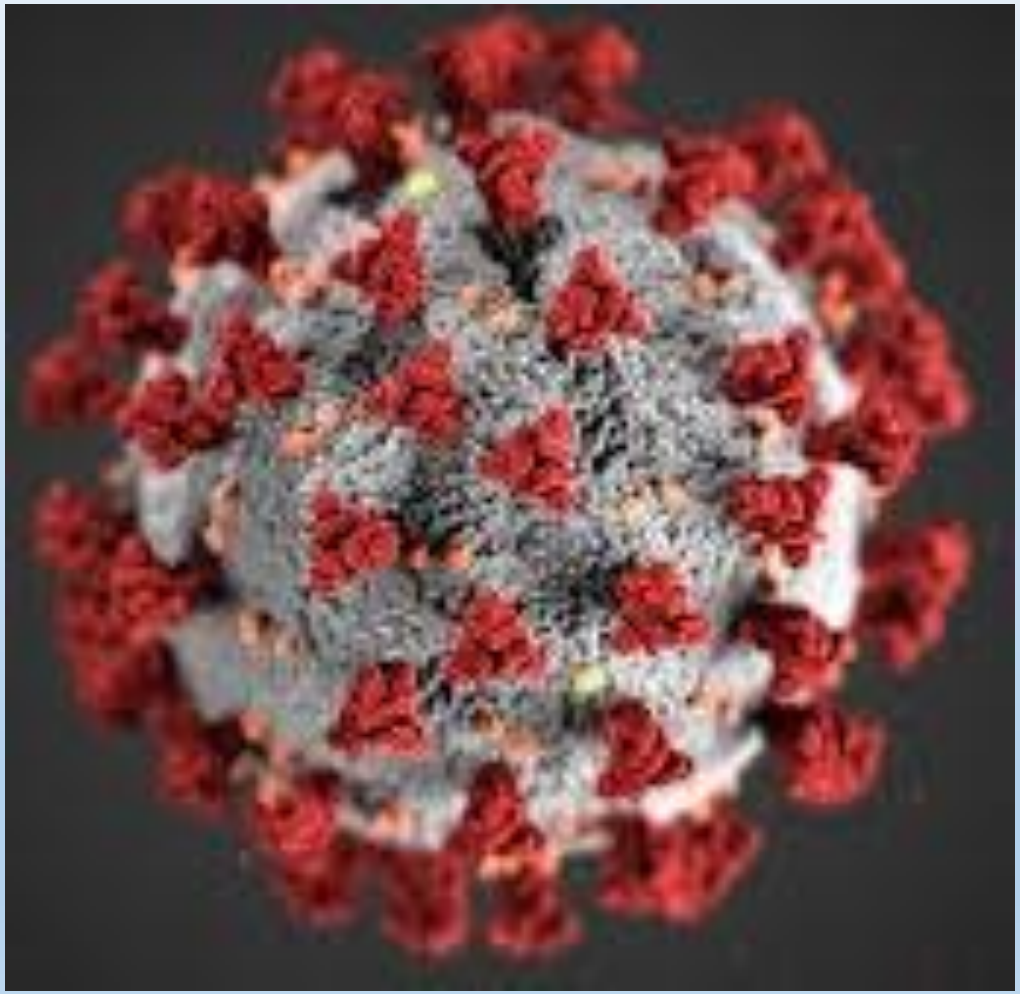
https://www.impactcybertrust.org/link_docs/Menlo-Report-Companion.pdf

- Ethics Codes
  - IEEE/ACM Codes
  - Association of Internet Researchers
  - National Academy of Sciences
  - SAFE/LPS SA/USENIX- joint System Administrators Code of Ethics
  - Responsible disclosure guidelines –National Infrastructure Advisory Council
  - Internet Advisory Board Guidelines - IETF

A Recent Case Study

- **GOOGLE**

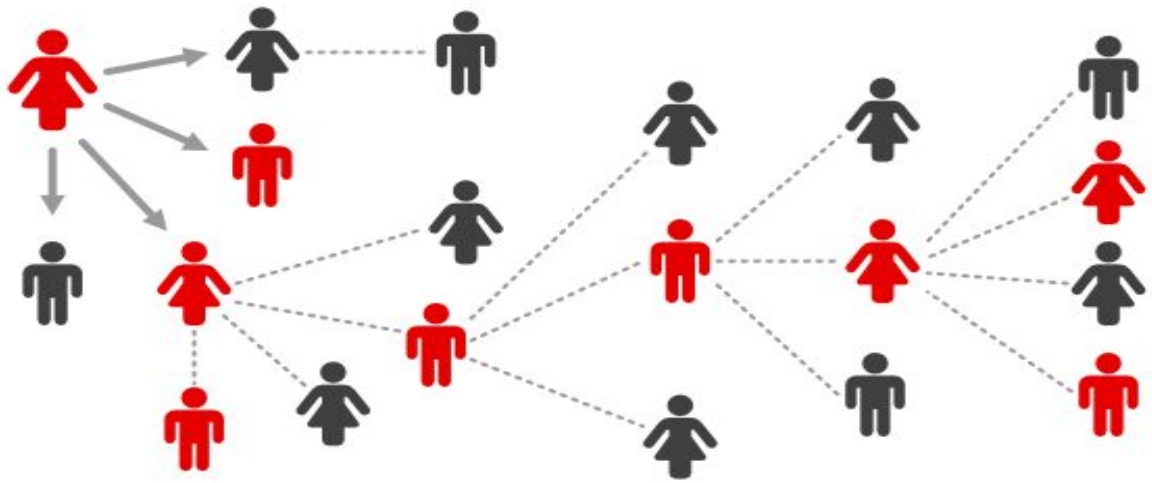
APPLE



Contact Tracing via Cell Phone

- Contact Tracing App
  - Requires activation
  - Voluntary, but…
- Contact Tracing via CSLI
  - Involuntary/voluntary
  - Data matching against public health databases and associational/GPS data
  - May require legal authority to do so

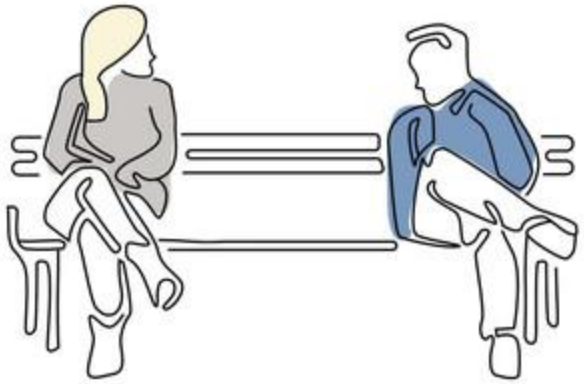
What is contact tracing?



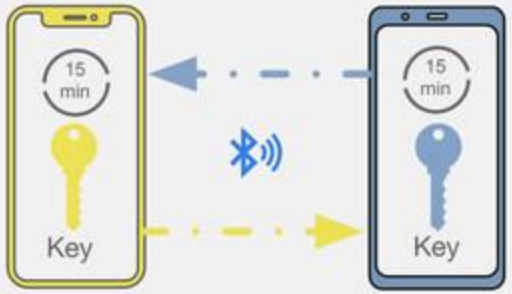
Contact tracing aims to identify and alert people who have come into contact with a person infected with coronavirus.

Smartphones can be used to quickly and automatically determine whether somebody has been in contact with an infected person.

Alice and Bob meet each other for the first time and have a 10-minute conversation.



Their phones exchange anonymous identifier beacons (which change frequently).



A few days later...

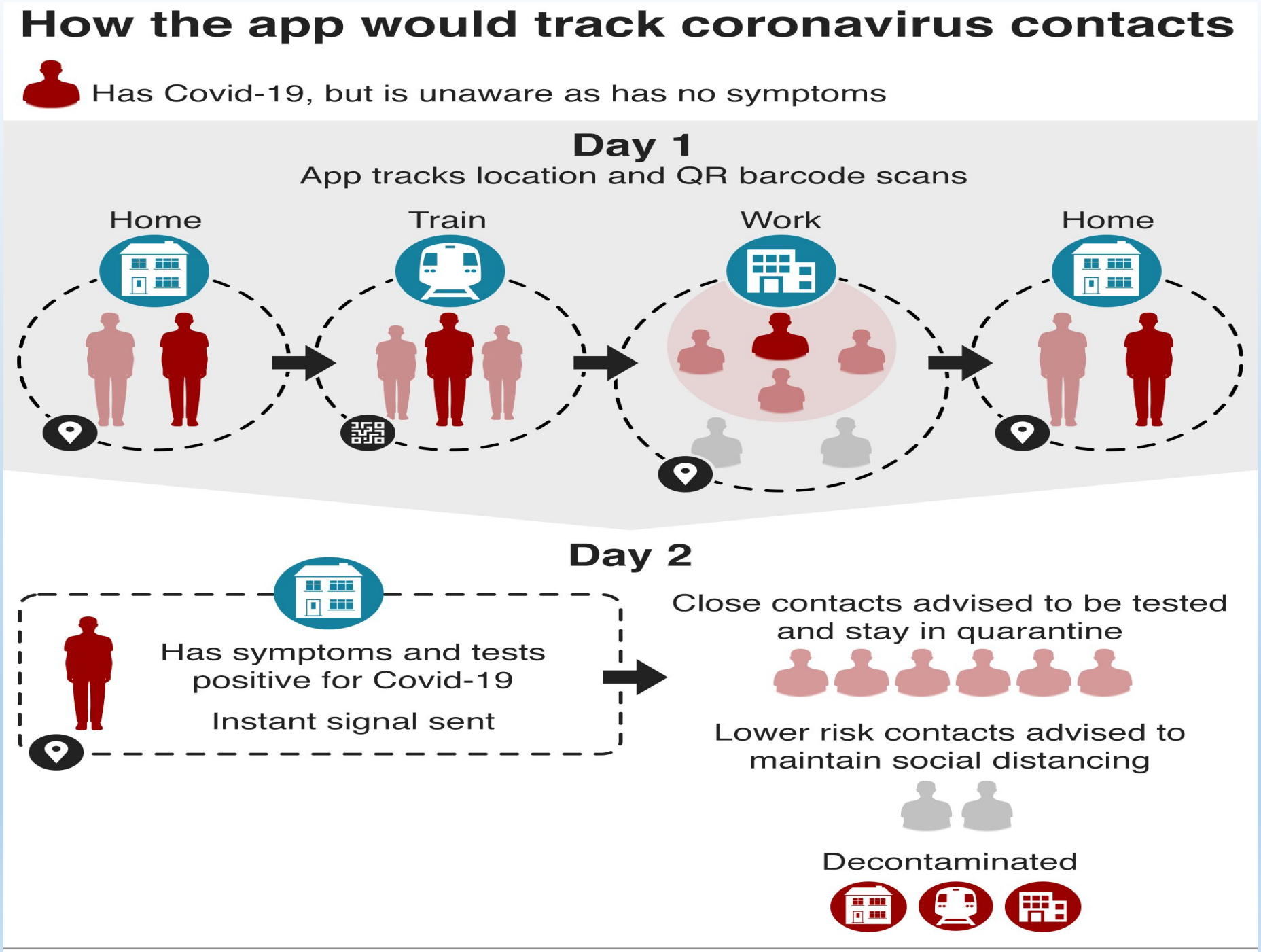
Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.

With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

Apps can only get more information via user consent

~14 day temporary store

Google


How the app would track coronavirus contacts
Has Covid-19, but is unaware as has no symptoms
Day 1
App tracks location and QR barcode scans
Home
Train
Work
Home
Day 2
Has symptoms and tests positive for Covid-19
Instant signal sent
Close contacts advised to be tested and stay in quarantine
Lower risk contacts advised to maintain social distancing
Decontaminated
Source: Oxford University
BBC

- Benefits?
  -
  -
- Risks?
  -
  -
  -
- Solutions?

What we will do now

- identify benefits of computing systems and resources within IoT
  -
  -
  -
- Identify risks of IoT
  -
  -
  -
- allocate responsibility for the use and misuse of computing and ICT within IoT
  - ✔
  - ✔
  - ✔
- apply techniques to protect the rights and the benefits of computing and ICT within IoT
  - ❖
  - ❖
  - ❖

Final Thoughts on AI, IoT, Ethics and Human Rights?

Citations

- Durer, Albrecht, “The Four Horsemen of the Apocalypse,” woodcut, ca. 1497-1498, image donated to Wikimedia Commons as part of a project by the National Gallery of Art (US)

- Goldsmith, Jack "The Failure of Internet Freedom," Emerging Threats, Knight First Amendment Institute, https://knightcolumbia.org/sites/default/files/content/Emerging_Threats_Goldsmith.pdf Accessed 25 May 2019
- Yemini, Moran, "The New Irony of Free Speech," 20 Columbia Science and Technology Law Review 119 (2018)
- *Google Inc. v. Hood,* 822 F.3d 212 (CA5 2016) (US)
- For content related regulation of speech there must be a compelling interest at stake, an effective regulation and no less strict avenues available to protect that compelling interest. Speech deemed not protected speech, such as obscenity and defamation, receives no protection.
- *US DOJ vs Apple, Inc*.

- Losavio and Losavio, *Information Crisis*, 2nd ed, InfoBase Publishing, New York, New York (2018)
- *Reno vs American Civil Liberties Union*, 521 US 844 (1997), citing *ACLU versus Reno*, 920 F.Supp.at 842 (1996)
- *"Congress shall make no law . . . abridging the freedom of speech." U. S. Const., Amdt. 1*
- Internet World Stats, *Usage and Population Statistics*, March 31, 2019, https://www.internetworldstats.com/stats.htm, accessed May 13, 2019
- United Nations News, "Internet milestone reached, as more than 50% go online: UN telecoms agency," 7 December 2018, https://news.un.org/en/story/2018/12/1027991, accessed May 13, 2019
- But some contends this masks a greater extent of underutilization due to costs, deployment and culture for the most vulnerable populations who might benefit from these technologies. Dreyfuss, Emily, "Global Internet Access Is Even Worse Than Dire Reports Suggest," Wired, October 23, 2018.
- Dow Jones And the Special Libraries Association, "Bad info: Unreliable Information from Web Leads Many Businesses to Bad Decisions, Missed Opportunities According to Survey," (2011)
- The Four Horsemen of the Apocalypse

- But see Cimpanu, Catalin, “In a first, Israel responds to Hamas hackers with an air strike,” ZDNet, US Edition, May 5, 2019, https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/ , accessed May 13, 2019
- Stark, Michael, "Kierkegaard for the Internet Age," Huffington Post, May 5, 2017
- *Milton, John, 1608-1674. (1971). Areopagitica. [New York] :[AMS Press],*
- Hobbes, Thomas, 1588-1679 *Leviathan, or, The matter, form, and power of a commonwealth, ecclesiastical and civil*. Baltimore: Pink and Books, 1968
- Cybersecurity Law of 2017, Article 28 (Peoples’ Republic of China)
- M. Losavio, C. Rogers and A. Elmaghraby, "Digital heritage from the Smart City and the Internet of Things: History or stasis?," *2015 Digital Heritage*, Granada, 2015, pp. 431-434. doi: 10.1109/DigitalHeritage.2015.7419541
- Walden, Matt, "Singapore's new anti-fake news law criticized as ’Orwellian’ threat to freedom of speech," ABC news Australia, 14 May 2019, https://www.abc.net.au/news/2019-05-14/singapore-fake-news-law-threatens-free-speech-say-critics/11111946, accessed May 17, 2019
- *New York Times v. Sullivan,* 376 U.S. 254 (1964)
- *Packingham v. North Carolina,* 137 S. Ct. 1730, 1773 582 US __, 198 L. Ed. 2d 273 – (2017) “…the internet offers an unprecedented degree of anonymity and easily permits a would-be molester to assume a false identity. The Court is correct that we should be cautious in applying our free speech precedents to the internet. Ante, at 1736"
- Freedom House, "Attacks on the Record: The state of global press freedom 2017-2018," https://freedomhouse.org/report/special-reports/attacks-record-state-global-press-freedom-2017-2018 accessed 17 May 2019
- *See Backpage.com, LLC v. Dart, 807 F.3d 229 (7th Cir.2015)* (holding unconstitutional a sheriff's threats to credit card companies to stop doing business with a website that hosts classified ads for prostitution)
- As the federal Fifth Circuit noted, Congress's grant of "broad immunity" to internet service providers "for all claims stemming from their publication of information created by third parties," which we and other circuits have consistently given a wide scope. *Doe v. MySpace, Inc.,* 528 F.3d 413, 418 (5th Cir. 2008)

- *Doe v. Backpage.com, LLC,* 817 F.3d 12, 18-24, 29 (1st Cir.2016) (affirming dismissal based on section 230 despite appellants' "persuasive case" that the defendant "tailored its website to make sex trafficking easier." That court stated further "If the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation."
- The resolution of an Internet bad content/ threats case *United States v Elonis* 135 S. Ct 2001 (2015) was treated not as a first amendment issues, but one of intent to threaten where the failure of the scienter element led to the reversal of the conviction. The Supreme Court noted that the "presumption in favor of a scienter requirement should apply to *each* of the statutory elements that criminalize otherwise innocent conduct." *X-Citement Video,* 513 U.S., at 72, 115 S.Ct. 464 (emphasis added). Elonis's conviction, however, was premised solely on how his posts would be understood by a reasonable person and thus inconsistent with "the conventional requirement for criminal conduct—*awareness* of some wrongdoing." *Staplesv. United States,* 511 U.S., 600, at 606-607, 114 S.Ct. 1793 (quoting *United States v. Dotterweich,* 320 U.S. 277, 281, 64 S.Ct. 134, 88 L.Ed. 48 (1943);
- See, Center for Democracy and Technology, "CDT Opposes Latest Threat to Host of Online Content, February 22, 2018, https://cdt.org/press/cdt-opposes-latest-threat-to-hosts-of-online-content/ accessed 25 May 2019
- see *Reno v. American Civil Liberties Union,* 521 US 844, 874 (1997) ("In evaluating the free speech rights of adults … The freedom of speech has its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity, and pornography …
- Kelly, Walt, "We Have Met the Enemy and He is Us," Pogo, Post-Hall Syndicate, April 22, 1970