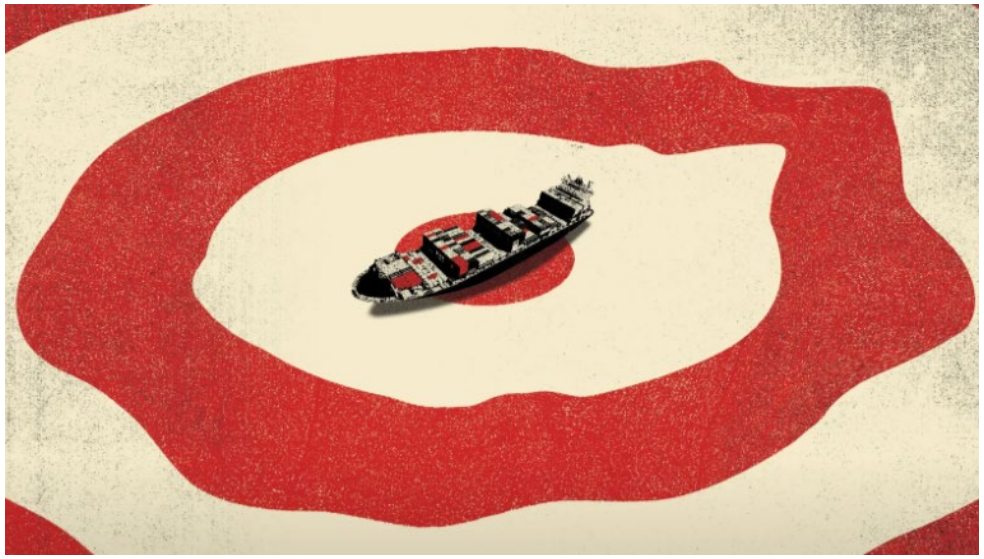
MSBA 5507.1 Ethics, Risk Management and Data Security

Incident Response, Data Ethics Frameworks and Professional Responsibility
August 7, 2022

Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, August 22, 2018



© Wired

$300,000,000
Danish shipping company Maersk

The release of NotPetya was an act of cyberwar . . . The weapon's target was Ukraine. But its blast radius was the entire world. "It was the equivalent of using a nuclear bomb to achieve a small tactical victory,"

After a frantic global search, the admins finally found one lone surviving domain controller in a remote office—in Ghana.

Rebuilt its entire network of 4,000 servers and 45,000 PCs.

Ken DeJarnette
ken@kdejarnette.com
ken.dejarnette@dominican.edu
213-399-8706
Office hours: Wed 1-3 pm by appointment

TOPIC	DESCRIPTION/SOURCES
Recap	Data acquisition

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

v.

CENTER FOR COUNTERING DIGITAL HATE, INC., a Washington, D.C. non-profit corporation; CENTER FOR COUNTERING DIGITAL HATE LTD., a British non-profit organization; and DOES 1 through 50, inclusive,

Defendants.

Case No.

COMPLAINT FOR:

(1) BREACH OF CONTRACT

(2) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

(3) INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONS; AND

(4) INDUCING BREACH OF CONTRACT

"CCDH has engaged in a series of ***unlawful acts to secure data*** regarding X that CCDH could then mischaracterize in its reports and articles alongside calls for companies not to advertise on X"

"intentionally sought and ***obtained unauthorized access to data*** sets regarding X"

"CCDH, as a registered user of the X service, also ***breached*** its agreement with X Corp., i.e., the ***Terms of Service*** ("ToS"), which ***expressly prohibit "scraping" without X's "prior consent."***

"CCDH's February 9, 2023 report ***admits to scraping X to obtain data for the report***, in which CCDH uses its manufactured and inaccurate narrative to openly call for companies to not advertise on X"

"As a direct and proximate result of CCDH US's ***breaches of the ToS in scraping X, X Corp. has suffered monetary and other damages*** in the amount of at least tens of millions of dollars . . ."

TOPIC	DESCRIPTION/SOURCES
Incident response	iPremier Case Study
Discussion	❑ Why wasn't iPremier prepared? What do you think drives preparedness or non-preparedness? ❑ When addressing a crisis, is it important to have principles? What are examples of principles? ❑ What key priorities should iPremier have established? ❑ What should iPremier communicate to its stakeholders (employees, customers, partners, investors)? ❑ What should iPremier do after the attack?

TOPIC	DESCRIPTION/SOURCES
Frameworks	*Principles for Accountable Algorithms and a Social Impact Statement for Algorithms*, Fairness, Accountability and Transparency in Machine Learning (FAT/ML)

Discussion

Principles

Underlying premise: *"There is always a human ultimately responsible for decisions made or informed by an algorithm."*

- ❑ **Responsibility**
  - ✓ "*Make available externally visible avenues of redress* for adverse individual or societal effects of an algorithmic decision system and designate an internal role for the person who is responsible for the timely remedy of such issues."
- ❑ **Explainability**
  - ✓ "Ensure that algorithmic decisions as well as any data driving those *decisions can be explained to end-users* and other stakeholders in non-technical terms."
- ❑ **Accuracy**
  - ✓ "Identify, log, and articulate sources of error and uncertainty throughout the algorithm and its data sources so that expected and worst-case implications can be understood and inform mitigation procedures."
- ❑ **Auditability**
  - ✓ "Enable interested third parties to probe, understand, and review the behavior of the algorithm through *disclosure of information that enables monitoring, checking, or criticism*, including through provision of detailed documentation, technically suitable APIs, and permissive terms of use."
- ❑ **Fairness**
  - ✓ "Ensure that algorithmic *decisions do not create discriminatory or unjust impacts* when comparing across different demographics (e.g., race, sex, etc.)."
- ❑ **Privacy**
  - ✓ Should be included and FAT/ML believe it is well covered in other guidance

TOPIC	DESCRIPTION/SOURCES
Frameworks	Questions to Ask: *Principles for Accountable Algorithms and a Social Impact Statement for Algorithms*, FAT/ML *See also* Data Ethics Framework, UK Government Digital Services

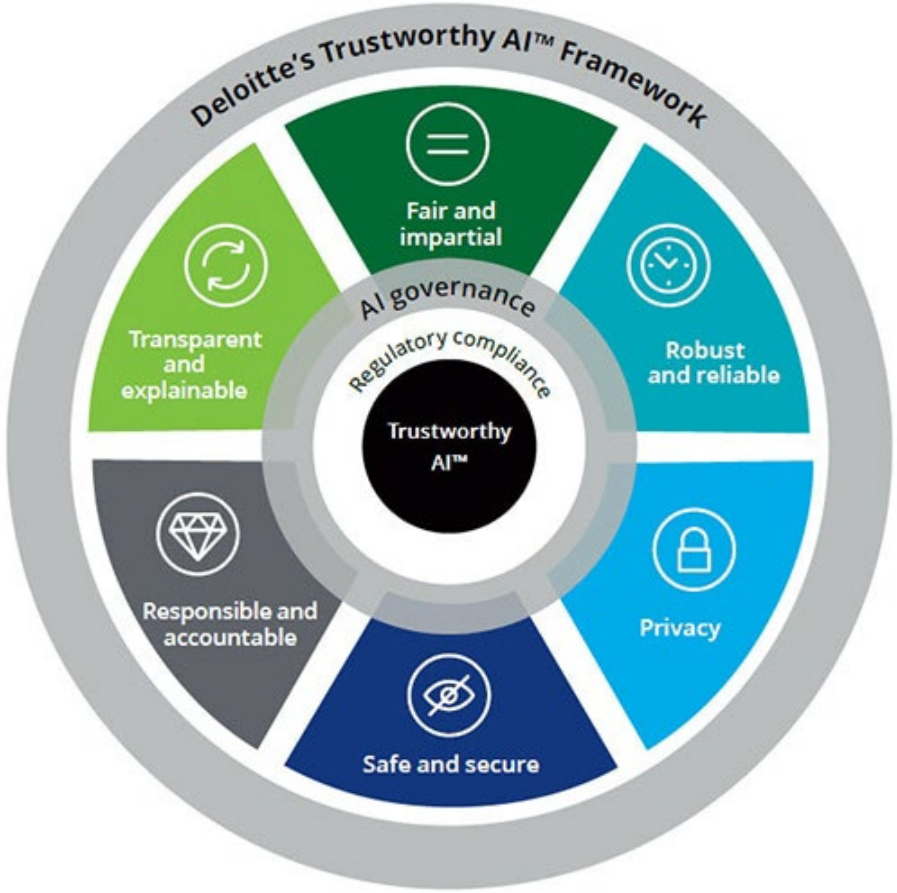
Discussion

Fairness, Accountability and Transparency in Machine Learning

- ❑ **Responsibility**
  - ✓ Who is responsible if users are harmed by this product?
  - ✓ What will the reporting process and process for recourse be?
  - ✓ Who will have the power to decide on necessary changes to the algorithmic system during design stage, pre-launch, and post-launch?
- ❑ **Explainability**
  - ✓ Who are your end-users and stakeholders?
  - ✓ How much of your system / algorithm can you explain to your users and stakeholders?
  - ✓ How much of the data sources can you disclose?
- ❑ **Accuracy**
  - ✓ What sources of error do you have and how will you mitigate their effect?
  - ✓ How confident are the decisions output by your algorithmic system?
  - ✓ What are realistic worst-case scenarios in terms of how errors might impact society, individuals, and stakeholders?
  - ✓ Have you evaluated the provenance and veracity of data and considered alternative data sources
- ❑ **Fairness**
  - ✓ Are there particular groups which may be advantaged or disadvantaged, in the context in which you are deploying, by the algorithm / system you are building?
  - ✓ What is the potential damaging effect of uncertainty / errors to different groups?
- ❑ **Auditability**
  - ✓ Can you provide for public auditing (i.e., probing, understanding, reviewing of system behavior) or is there sensitive information that would necessitate auditing by a designated 3rd party?
  - ✓ How will you facilitate public or third-party auditing without opening the system to unwarranted manipulation?

Frameworks *Trustworthy AI*, Deloitte (2021)

- ❑ **Fair and impartial**
  - ✓ "Assess whether AI systems include internal and external checks to help enable equitable application across all participants."
- ❑ **Transparent and explainable**
  - ✓ "Help participants understand how their data can be used and how AI systems make decisions. Algorithms, attributes, and correlations are open to inspection."
- ❑ **Responsible and accountable**
  - ✓ "Put an organizational structure and policies in place that can help clearly determine who is responsible for the output of AI system decisions."
- ❑ **Robust and Reliable**
  - ✓ "Confirm that AI systems have the ability to learn from humans and other systems and produce consistent and reliable outputs."
- ❑ **Respectful of privacy**
  - ✓ "Respect data privacy and avoid using AI to leverage customer data beyond its intended and stated use. Allow customers to opt in and out of sharing their data."
- ❑ **Safe and secure**
  - ✓ "Protect AI systems from potential risks (including cyber risks) that may cause physical and digital harm."



TOPIC	DESCRIPTION/SOURCES
Frameworks	Jessica Fjeld et al., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, The Berkman Klein Center (2020)

The principles within each theme are:

Privacy:
Privacy
Control over Use of Data
Consent
Privacy by Design
Recommendation for Data Protection Laws
Ability to Restrict Processing
Right to Rectification
Right to Erasure

Accountability:
Accountability
Recommendation for New Regulations
Impact Assessment
Evaluation and Auditing Requirement
Verifiability and Replicability
Liability and Legal Responsibility
Ability to Appeal
Environmental Responsibility
Creation of a Monitoring Body
Remedy for Automated Decision

Safety and Security:
Security
Safety and Reliability
Predictability
Security by Design

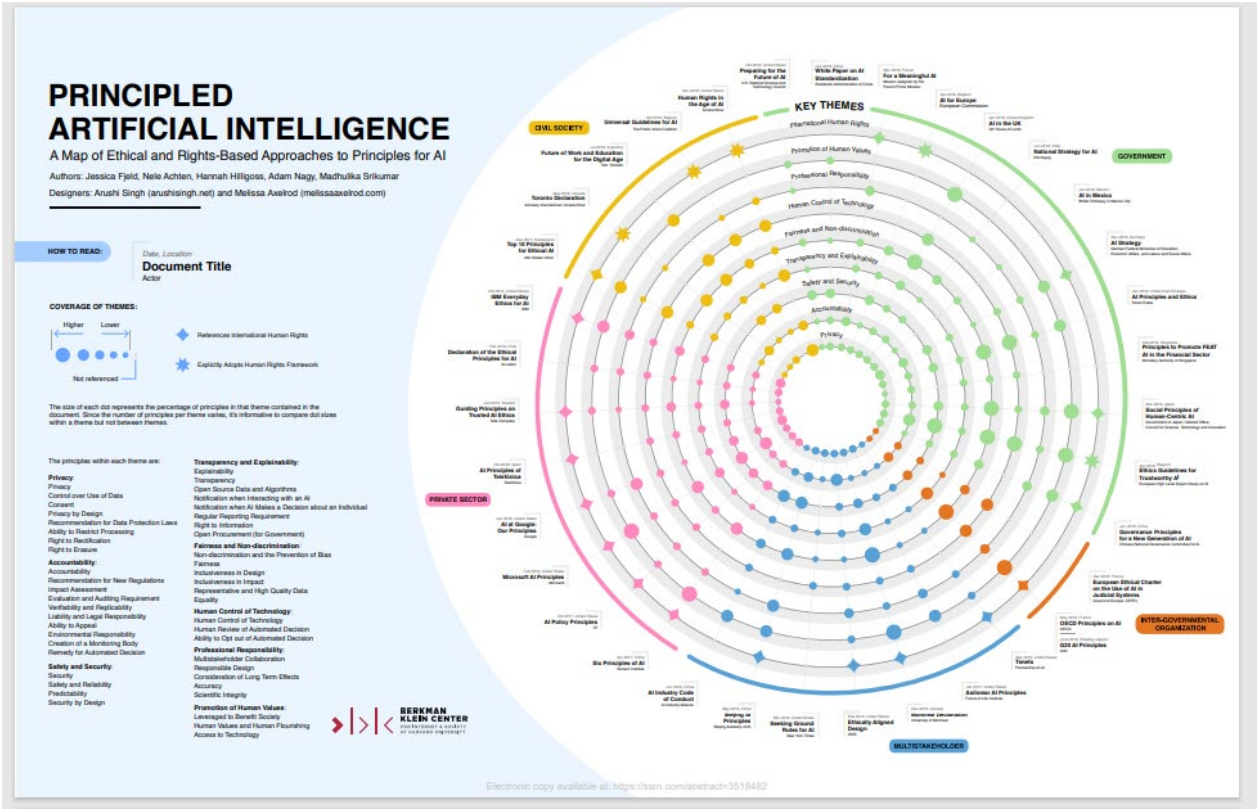
Transparency and Explainability:
Explainability
Transparency
Open Source Data and Algorithms
Notification when Interacting with an AI
Notification when AI Makes a Decision about an Individual
Regular Reporting Requirement
Right to Information
Open Procurement (for Government)

Fairness and Non-discrimination:
Non-discrimination and the Prevention of Bias
Fairness
Inclusiveness in Design
Inclusiveness in Impact
Representative and High Quality Data
Equality

Human Control of Technology:
Human Control of Technology
Human Review of Automated Decision
Ability to Opt out of Automated Decision

Professional Responsibility:
Multistakeholder Collaboration
Responsible Design
Consideration of Long Term Effects
Accuracy
Scientific Integrity

Promotion of Human Values:
Leveraged to Benefit Society
Human Values and Human Flourishing
Access to Technology



TOPIC	DESCRIPTION/SOURCES
Professional Responsibilities	*Data Science Code of Professional Conduct,* Data Science Association

Discussion

- ❑ Rule 1 - Terminology
- ❑ Rule 2 - Competence
- ❑ Rule 3 - Scope of Data Science Professional Services Between Client and Data Scientist
- ❑ Rule 4 - Communication with Clients
- ❑ Rule 5 - Confidential Information
- ❑ Rule 6 - Conflicts of Interest
- ❑ Rule 7 - Duties to Prospective Client
- ❑ **Rule 8 - Data Science Evidence, Quality of Data and Quality of Evidence**
- ❑ Rule 9 - Misconduct

(d) If a data scientist **reasonably believes a client is misusing data science to communicate a false reality or promote an illusion of understanding**, the data scientist **shall take reasonable remedial measures**, including disclosure to the client, and including, if necessary, disclosure to the proper authorities. The data scientist shall take reasonable measures to persuade the client to use data science appropriately.

See also, IFIP Code of Ethics and Professional Conduct and *ACM Code of Ethics and Professional Conduct*

TOPIC	DESCRIPTION/SOURCES
Certifications	iapp.org isc2.org isaca.org
Discussion	The International Association of Privacy Professionals (IAPP) ❑ Certified Information Privacy Professional (CIPP) ❑ Certified Information Privacy Manager (CIPM) ❑ Certified Information Technology Professional (CITP) International Information System Security Certification Consortium $(ISC)^2$ ❑ Certified Information Systems Security Professional (CISSP) Information Systems Audit and Control Association (ISACA) ❑ Certified Information Security Auditor (CISA) ❑ Certified in Risk and Information Systems Control (CRISC) ❑ Certified Information Security Manager (CISM)