Surveillance, Privacy and Data

Stefan Dobre
Critical Algorithm Studies SS16

Ends And Ways: The Algorithmic Politics of Network Neutrality

McKelvery, Fenwick 2010

The definitions

- Net neutrality
- Critics
- Quality of Service vs End-to-End

Network neutrality advocates demand packet quality where all packets transmitted over the public Internet be treated equally, regardless of source, ownership, content, or destination

The definitions

- Net neutrality
- Critics
- Quality of Service vs End-to-End

2 types of algorithms

E2E

A best effort behind end to end algorithms amounts to networks avoiding any knowledge of the contents of the packets and focusing on routing the packet to its final destination.

TCP-IP

The problem:

Bandwidth hungry applications, at the expense of time sensitive interactive applications.

56% of all Traffic

QoS

The network relations of Quality of Service manage bandwidth to ensure certain channels of communication receive sufficient resources to guarantee their successful operation.

Critics: Such a system guarantees quality of service to ‘premium’ users and prioritize services, even at times of major internet congestion.

“We have to manage traffic to ensure that p2p file sharing applications on the internet do not impair the quality of our services.”

“… to prevent congestion, and promote value-added services.”

Growth of QoS

DPI

Deep packet inspection

Monitors all 4 layers of the package (including the message)
Pattern recognition and packet storage

DFI

Deep flow inspection

Inspection of rate of incoming data. (skype)

Examples

Wilhelm.tel – bandwidth limitation

Bell Canada – BitTorrent

Value Added Services:

- Cogego offers prioritized VoIP
- Rogers has video on demand
- Bell offers streaming TV

Algorithmic War: Everyday Geographies of the War on Terror

Louise Amoore 2011

Background

Statements:

- Only 5 month after 9/11, IBM’s federal business manager testified that “in this war, our enemies are hiding in the open and available information across a spectrum of databases”
- If we learned anything from September 11, it is that we need to be better at connecting the dots of terrorist-related information.
- In 2003, a US joint inquiry concluded that “on September 11, enough relevant data was resident in existing Databases”, so that “had the dots been connected”, the events could have “exposed and stopped”

Main claim

“The significant point here is that probabilistic knowledge, based on the database residue of daily life, becomes a means of securitization”

Use of existing technology

Example:

- Oracle
- Algorithmic security systems for the entertainment industry and used in Las Vegas casinos -> deployed by US Justice and fedetal intelligence for counter terror
- Non-Obvious Relationship Awareness- NORA searches for behaviour patterns or personal associations that hint at terrorist activities, turning data into actionable intelligence

Information + Consequence

Information collected:

- Concerning a suspect, it is looked into: was the ticket paid in cash? Was is the last pattern of travel? Is this a frequent flier? What in-flight meal was ordered?

Consequences:

- If suspicous activity was detected, it may result in: detention at international borders, freezing of financial assets, interception of cargo at ports

The precautionary principle

- Algorithmic Security technologies allow the embracing of the precautionary principle, inviting anticipatory actions and making scientific and certain what would otherwise be mere uncertain doubts or suspicions

- UK’s metropolitan Police

The problem that arises

The figure of enmity to be feared and intercepted need not only dwell in a represented outside in the geographies of Iraq and Afghanistan, for the outside can be inside.

“One does not know on which face of the strip one is located”

Algorithmic logics appear to make it possible to translate probable associations between people and objects into actionable security decisions, or to incorporate the uncertain future into the present.

3 blog articles

China's "Unified Information Environment"

Input:

online behavior, financial transactions, work data, calls, travel etc.

Wants to Detect:

anything from terror attacks to major gatherings of people

How it's possible:

"domestic security and stability" budget surpasses national security.
terrorism laws force businesses to provide assistence in surveilling.

Hidden Biases in Big Data

Hurricane Sandy

20mil Tweets. Made it look like NY was most impacted. "signal problem"

Boston potholes

Streetbump app.
Lower income communities, the elderly have no less access.

Google Flue Trends

False due to hype caused by mass media.

Bing and Google autocomplete

Google:

"We exclude a narrow class of search quaries related to pornography, violence, hatespeech and copyright infridngement."
They don't suggest a lot.

Bing:

"We filter spamand block adult or offensive content"
They prend dirty words a typos.

Accidents/Errors:

THANKS
for your attention!