Could Anders Behring Breivik have been stopped with social media monitoring?

VOXPol - Ethics and Politics of Online Monitoring of Violent Extremism

Brussels January 19, 2015

Dr. Robindra Prabhu

Norwegian Board of Technology
Security and openness post July 22, 2011

- Public debate on internet surveillance after July 22, 2011
- “Open” policing:
  - Social media surveillance
  - Predictive policing
“Our answer to violence is more openness, more democracy...but we will not be naïve.”

Prime Minister Jens Stoltenberg
“Our answer to violence is more openness, more democracy…but we will not be naïve.”

Prime Minister Jens Stoltenberg

Anonymity online?

http://www.aftenposten.no/meninger/kommentarer/Farvel_anonymitet-7983457.html
“Our answer to violence is more openness, more democracy... but we will not be naïve.”

Prime Minister Jens Stoltenberg

Anonymity online? Internet trolls?

http://www.aftenposten.no/meninger/kommentarer/Farvel_anonymitet-7965457.html

http://www.dubestemm er.no/content/trollus-netticus
“Our answer to violence is more openness, more democracy...but we will not be naïve.”

Prime Minister Jens Stoltenberg

Anonymity online? Internet trolls? Internet surveillance?

http://www.aftenposten.no/meninger/kommentarer/Farvel_anonymitet-795407.html

http://www.dubestemner.no/content/trollus-netticus

Could Anders Behring Breivik been stopped through tighter monitoring of his online activities?
Could Anders Behring Breivik been stopped through tighter monitoring of his online activities?

NO
Could Anders Behring Breivik been stopped through tighter monitoring of his online activities?

...probably not
The Online Life of a Modern Terrorist: Anders Behring Breivik's Use of the Internet

Did the Internet play a decisive role in Anders Behring Breivik's violent radicalisation? In a recent study of Breivik's online activities, I went through his posts on various message boards between 2002 and 2011, in addition to a collection of more than 7,000 of his private e-mails forwarded by Norwegian hackers to a Norwegian journalist six days after the terrorist attacks. I also attended Breivik's 2012 trial on a daily basis, which offered further insights into Breivik's Internet adventures and road to militancy.

My study led me to five main findings: First, Breivik never discussed his terrorist plans with anyone online. In fact, his online posts can hardly be described as extreme compared to some of the posts that appear regularly in the comments sections in mainstream news media. In other words, even if Norwegian Security Authorities had systematically monitored his online activity, it is unlikely that they would have responded.
…never discussed his terrorist plans online

…critical views on Islam and socialism where established long before counterjihad blogs were created

…only turned to violence after having been rejected by people he admired and wanted to work with

…prolonged withdrawal from family and friends (year off to play computer games) may have influenced radicalisation

…Internet gave him knowledge and ingredients to carry out attacks, but not necessarily the idea to attack
State of limbo...

Poorly adapted to the internet age:

- Should have prioritised internet-based OSINT to a much larger extent

- Should not “hold back” on the monitoring of extremist internet websites for fear of being criticised for political surveillance
PST: stuck between a rock and hard place?

- Proposal: collect & store “big data” for the purposes of aggregate analysis with aim to identify trends and future challenges
  - not drill down to the level of individuals

- proposal instantly shot down by both sides of the political divide

---

Terror attacks of July 22 and commission report

Rock

Hard place

Snowden revelations

Where do we go from here?

...let’s start with “open” policing
Police stations in Norway have had great success using social media as an effective information channel to the public.
…but can social media be used as an information channel to the police?
Analysis of the entire Twitter-feed on July 22, 2011
I think the police should monitor words like “shooting”, “explosion” and “fighting” on open social medias platforms like Twitter in order to discover new events.
I think the police should monitor words like “shooting”, “explosion” and “fighting” on open social medias platforms like Twitter in order to discover new events.
I think the police should monitor words like “shooting”, “explosion” and “fighting” on open social medias platforms like Twitter in order to discover new events.

If I knew that the police was monitoring certain words and expressions on social media, I would avoid using these words.
I think the police should monitor words like “shooting”, “explosion” and “fighting” on open social medias platforms like Twitter in order to discover new events.

If I knew that the police was monitoring certain words and expressions on social media, I would avoid using these words.
Open vs closed spaces online

1. Does technically open mean that it is public?
   - much of what we say is neither strictly private, nor strictly public

2. What is public?
   - The picture of latté art shared on social media or the metadata attached to it with location and time stamp?

3. Technically open is a moving target
   - Who has the defining power in what “public” means?
Key recommendations
Key recommendations

1. Use only open information - and be clear about what you consider to be “open”
Key recommendations

1. Use only open information - and be clear about what you consider to be “open”

2. Use only aggregate data for situational awareness - do not drill down to identify individuals unless you are in an investigation
Key recommendations

1. Use only open information - and be clear about what you consider to be “open”

2. Use only aggregate data for situational awareness - do not drill down to identify individuals unless you are in an investigation

3. Build in privacy preserving features from the start, eg. facial blurring
Computer algorithms predicting the **when**, **where** and **who** of the next crime...
“Through data analysis, Chicago police have identified more than 400 people they believe are most likely to drive up violent crime - as perpetrators or as victims - and are warning them”
From “hotspots” to “heat lists”

Potential future perpetrators / future victims

Homicide victims

Predictive analysis of social network around homicide victims inside hotspots

Selective attention is not new to policing...

...but how do we deal with the discomfort of whom to survey more closely when the technology allows for more granular risk assessments?
Threshold problem

Data conundrum

Framing problem
Resource allocation with “surgical precision”

Threshold problem

Data conundrum

Framing problem

…but reasonable cause for suspicion?
Resource allocation with “surgical precision”

Data-driven analysis curbs personal prejudice

Threshold problem

Data conundrum

Framing problem

...but reasonable cause for suspicion?

...or guilty by association?
1. Resource allocation with “surgical precision”

2. Data-driven analysis curbs personal prejudice

3. Are you at risk…

Threshold problem

1. …but reasonable cause for suspicion?

2. …or guilty by association?

3. …or a risk?

Data conundrum

Framing problem
Thanks!

robindra.prabhu@teknologiradet.no