

An exploration of the conceptual border between *mass* and *targeted* surveillance

Heidi Mork Lomell, University of Oslo & Norwegian Police University College¹

Abstract

In political debate on online surveillance measures in Norway, the conceptual distinction between mass and targeted surveillance is becoming increasingly central. In this paper, I will explore the underlying assumptions and consequences of this particular framing of the debate.

Both those that support and those that oppose new online surveillance measures often use this distinction, and they share the assumption that mass surveillance is bad because it targets innocent law-abiding citizens while targeted surveillance is good/better because it targets guilty offenders and/or terrorists. What they normally disagree on is whether the proposed measures entail targeted or mass surveillance.

Both sides seem to ignore the inherent problem of this shared assumption, namely that of sorting offenders from law-abiding citizens in the first place. In my paper, I will use insights from criminological research on preventive justice to challenge this conceptual distinction and its underlying assumptions.

Extended abstract

Introduction

My first meeting with the distinction between what is now usually conceptualized as mass surveillance (*masseovervåking*) and targeted surveillance (*målrettet overvåking*) in Norway, was in 2007, when the then head of the Norwegian police security service (PST), Jørn Holme, in a debate on counter terrorism surveillance measures stated that “We want to use a harpoon, not a trawl bag”.² He didn’t explain this further but assumed that the audience understood his message.

A harpoon is a long spear-like instrument or weapon used in fishing, whaling, sealing, and other marine hunting to catch large fish or marine mammals. It accomplishes this task by impaling the target animal and securing it with barb or toggling claws, allowing the fishermen to use a rope or chain attached to the butt of the projectile to catch the animal.³

¹ This research is part of the NordForsk-funded research project «Taking surveillance apart?: Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers» (project number 81105).

<https://www.nordforsk.org/en/programmes-and-projects/projects/taking-surveillance-apart-accountability-and-legitimacy-of-internet-surveillance-and-expanded-investigatory-powers>

² «Vi ønsker å bruke harpun, ikke trålpøse». PST har søkelyset rettet mot 200-300 personer. Dagsavisen, 26.9.2007

³ <https://en.wikipedia.org/wiki/Harpoon>

Trawls, also called “The bulldozers of the Ocean”, are enormous, cone-shaped fishing nets that are towed by one or two boats. As the net is towed, it herds and captures everything in its way, both fish and other creatures. Trawls are highly indiscriminate, capturing any and all species in their path. They catch high amounts of species that fishermen are not trying to catch, termed ‘bycatch’. The unintended catch or bycatch may include many species of fish, invertebrates (such as crabs, scallops, starfish or corals), sharks, skates and rays, endangered sea turtles, and sometimes whales and dolphins. Fishermen often throw much of this unintended catch back to sea dead or dying.⁴

When going fishing, using a harpoon means selecting your target first, and then aiming your weapon only at that target, while fishing with a trawl bag means catching everything in its range, and only afterwards sorting the intended from the unintended catch. When the head of the security police service uses these fishing techniques figuratively to illustrate the alternative methods at hand for the police, and the preferred measure, it is a powerful illustration and message to the public that harpoons are to be preferred in counter-terrorism policing, not trawls. The underlying assumption being that giving the police a harpoon will pose no risk to the innocent, law-abiding citizen, that the police are accurate (treffsikker), both when it comes to sorting the terrorist from the law-abiding citizen, and then accurate at hitting the target when shooting. Using a trawl will lead to loads of innocent people being caught in the net.

This way of illustrating how the PST works, was used for many years, mainly by the police service themselves. In 2009, head of information in PST, Martin Bernsen, stated that their work is “actor oriented” (aktørfokusert), which means that they do not surveille groups, only individuals. And to illustrate the security police’s approach, he continued; “We use a harpoon, not a trawl bag”.⁵

Today, “harpoon” has been replaced by “targeted surveillance”, and “trawl bag” has been replaced by “mass surveillance”. In this paper I want to look closer at the usage of these concepts in Norwegian surveillance debate. I will look closer at the conceptual border between mass and targeted surveillance, the underlying assumptions and finally the consequences of this particular framing of the debate.

Framing

The framing of a debate is crucial for people’s opinion. How the politicians, stakeholders and media frame a debate will also influence the legal and political decision-making. Not only the public, but also judges, lawmakers and stakeholders both use and are influenced by frames. Frames determines how we understand and remember a given problem or issue, as well as how we evaluate and choose to act upon it. Framing directs attention to particular aspects of a described reality, and by this, direct attention away from other facets. Frames are therefore not only important in what they include, but also by what they thereby exclude. The omissions may be as critical as the inclusions in guiding the audience.

According to Robert Entman, “To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem

⁴ <http://safinacenter.org/2015/02/fishing-gear-101-trawls-bulldozers-ocean/>

⁵ PST følger «i underkant av 200»: Færre overvåkes i Norge. ABC Nyheter, 13.11.2009

definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described.”⁶

In surveillance debate, the dominant frame pits security against privacy. This framing of the debate assumes that security and privacy are on the opposite sides of a scale, almost mutually exclusive. It assumes that if we want more security, we need to give up some privacy. The participants in the debate gets fixated on questions of *whether* privacy or security should be protected and/or privileged, at the expense of alternative approaches as to *how* privacy or security should be enhanced. All frames ignore alternative aspects of the reality of the debate⁷. Some dichotomies – and the privacy – security frame is a candidate here – may also be described as false. Thinking of surveillance measures only within the security/privacy frame or dichotomy, also ignores important aspects of current surveillance practices, such as social sorting and discrimination.⁸

Of course, the privacy – security frame is very much present and widespread also in Norwegian surveillance debate. However, following two recent surveillance debates in Norway, the first concerning a new law that was passed in 2016, allowing the Norwegian police to use “Data reading” (Dataavlesning) – meaning to enter a person’s digital device in order to monitor all activity, including reading all key strokes, the second concerning a proposal by the government to establish a “Digital border defence” (Digitalt grenseforsvar) – the monitoring of communications of foreign citizens over the fiber optic cables that crosses the Norwegian border, I was struck by another increasingly important framing: Mass v Targeted surveillance. In this paper, I will look at statements in these two surveillance debates which explicitly argues within the framing mass/targeted surveillance. First, let us look closer at the term mass surveillance and targeted surveillance.

Mass v. Targeted Surveillance

Mass or untargeted surveillance is the surveillance of all individuals in a specific place or engaged in a specific activity. Examples of mass or untargeted surveillance is security checks at airports, road traffic surveillance cameras and the monitoring of all data traffic crossing the national border. Mass surveillance is not restricted to known or suspected offenders. This is “trawling”, meaning that nobody is singled or sorted out, all are under “generalized suspicion”. Other concepts used as synonyms for mass surveillance in the literatures is untargeted surveillance, total surveillance and blanket surveillance.

Targeted surveillance, on the other hand, is surveillance directed at specific individuals or categories based on some sort of information of that individual or group of individuals. There is either individualized or categorical suspicion before the surveillance. This is “harpooning”.

Surveillance measures can be more or less targeted, and Hadjimatheou places individual/targeted and mass/untargeted surveillance at opposite ends of a spectrum.⁹ While targeted surveillance implies that an authority zones in on (or singles out) a group or individual from the total population,

⁶ Robert M. Entman (1993): Framing: Toward clarification of a fractured paradigm. In: Journal of communication, 51, 51.

⁷ Woodrow Hartzog (2013): The Fight to Fram Privacy. Michigan Law Review, Vol. 111:102.

⁸ Surveillance as social sorting: Privacy, risk and digital discrimination. Ed. by David Lyon. London: Routledge 2003.

⁹ Katerina Hadjumatheou (2014): «The relative moral risks of untargeted and targeted surveillance». In: Ethic Theory Moral Prac, vol 17:187-207.

untargeted surveillance does not involve zoning in or singling out. Untargeted surveillance “involve an authority surveilling everyone who falls under the auspices of that authority”.¹⁰

Between these two extremes, we find surveillance measures such as *profiling* and *randomized surveillance*. Profiling, as untargeted surveillance, affects groups and/or categories of people, but it differs in that it singles these groups out for suspicion based on characteristics. Randomized surveillance also singles out people, but, as the name indicates, the sorting is random, and not based on suspicion. One example can be randomized drug tests at sports competitions.

Maras claims that the 2004 Madrid and 2005 London bombings led to a larger shift in Europe from targeted to mass surveillance.¹¹ A prominent example of this was the Data Retention Directive issued by the European Union in 2006, which obliged Member States to require operators to collect and retain all telecommunications traffic data. The Snowden revelations further exposed the scale of this trend toward mass surveillance of ordinary citizens. Both the Data Retention Directive and the Snowden revelations were debated also Norway, and the terms “mass” and “targeted” surveillance established themselves in the general surveillance discourse and became an important frame in the debate.

Norwegian surveillance debate

I have analysed statements made in two debates on online surveillance in Norway. The first concerned new legislation that was finally enacted in 2016 concerning the police method “Data reading” (in Norwegian: Dataavlesning, see above). The second is still ongoing, and it concerns what is called “Digital border defence” (in Norwegian: Digitalt grenseforsvar, see above). The surveillance measures are by some seen as illustrative of respectively targeted surveillance (Data reading) and mass surveillance (Digital border defence) – but not all agree on that.

In my presentation I will analyse the following statements in order to tease out underlying assumptions in the targeted/mass framing of surveillance.

Digital border defence

“It will collect a lot of personal data, and the very vast majority do not pose a threat to society. The proposal does, in our opinion, violate constitutional rights on private communication and private life itself. The collection of data is simply not targeted, Thon says to VG.”¹²

“Communication control in an ‘interferenist’ form based on a non-existent suspicion, is principally very questionable. Compared to crime control, where gathering of information by means of surveillance is targeted at people who are de facto suspects of crime, the intelligence service’s retrieval appears to be of a general nature.”¹³

¹⁰ Ibid, p. 201.

¹¹ Marie-Helen Maras (2013): From targeted to mass surveillance: Is the E.U. Data Retention Directive a Necessary Measure or an Unjustified Threat to Privacy? In: *New Directions in Surveillance and Privacy*. Ed. by B. J. Goold and D. Neyland.

¹² - Dette vil samle mye personopplysninger, og de aller, aller fleste utgjør ingen trussel mot samfunnet. Forslaget strider derfor etter vår mening mot grunnlovsvernet rundt privat kommunikasjon og selve privatlivet. Innsamlingen er rett og slett ikke målrettet, sier Thon til VG. *Frykter dataangrep mot Stortingsvalget*. VG, 21.01.2017.

¹³ Kommunikasjonskontroll i en inngripende form med utgangspunkt i et mistankegrunnlag som ikke eksisterer, er prinsipielt meget betenkelig. Sammenlignet med bekjempelse av kriminalitet hvor innhenting ved bruk av overvåking som virkemiddel skjer målrettet mot personer som det er et de facto mistankegrunnlag mot,

“Digital Border Defence does not imply that the intelligence service will monitor ordinary people's emails, telephone traffic or internet surfing. It is not a matter of mass surveillance, but targeted searches in selected cross-border data streams.”¹⁴

“The first and most important objection to Digital Border Defence is that it allows for mass surveillance.”¹⁵

“The Judges Association agrees with the committee that it is a highly interventional communication control based on *non-existent suspicion*. Contrary to the fight against crime where surveillance is targeted at a suspected person, the intelligence service's surveillance will be more general.”¹⁶

Data Reading

“Data reading is a targeted measure that can prevent terrorism.”¹⁷

Bjørnland emphasizes that the Police security service will need an approval from court before they can start reading someone's keyboard and that the system will not be used for mass surveillance. - Data reading will be a tool that in each case requires a legal approval based on a concrete suspicion. It will be a "targeted" tool aimed at individuals and not a mass surveillance tool.”¹⁸

“Thon in the Data Inspectorate points out that there must be a clear distinction between mass surveillance and proper surveillance against individuals suspected of intent to commit serious criminal acts.”¹⁹

Underlying assumptions

Mass surveillance is bad, targeted surveillance is good/better.

fremstår E-tjenestens innhenting til å være av en generell art. *Mistenkt til det motsatte er bevist?* Stavanger Aftenblad, 16.2.2017

¹⁴ DGF innebærer ikke at E-tjenesten vil overvåke vanlige menneskers e-poster, telefontrafikk eller internettsurfing. Det er ikke tale om masseovervåking, men målrettede søk i utvalgte grenseoverskridende datastrømmer. *Misvisende om digitalt grenseforsvar*. Aftenposten, 18.1.2017

¹⁵ Den første og viktigste innvendingen mot DGF er at det åpner for masseovervåking. *Det er grunn til å advare mot at E-tjenesten og PSTs trusselvurdering blir for dominerende som premisseleverandør for det offentlige ordskiftet*. VG, 19.2.2017

¹⁶ Dommerforeningen er enig med utvalget i at det er tale om en svært inngripende kommunikasjonskontroll basert på et ikke-eksisterende mistankegrunnlag. I motsetning til kriminalitetsbekjempelse der innhenting ved overvåking foregår målrettet mot noen som man har et mistankegrunnlag mot, så er E-tjenestens virksomhet mer generell. (Dommerforeningen høringssvar)

¹⁷ Dataavlesning er et målrettet verktøy, som kan forhindre terrorisme. *Nei til dataavlesning*. Bergens Tidene, 17.4.2017

¹⁸ Bjørnland er opptatt av å understreke at PST vil trenge en godkjenning fra retten, før de eventuelt kan starte å lese av noens tastatur, og at ordningen ikke skal kunne brukes til masseovervåking. - Dataavlesning vil være et virkemiddel som i hvert enkelt tilfelle forutsetter en rettslig kjennelse med utgangspunkt i et konkret mistankegrunnlag. Det vil være et "spisst" virkemiddel, rettet mot enkeltindivider og ikke et verktøy for omfattende overvåking. *Prioriterer islamister over høyreekstreme*. Dagsavisen, 17.7.2015

¹⁹ Thon i Datatilsynet peker på at det må være et klart skille mellom masseovervåking og korrekt overvåking mot enkeltpersoner som det foreligger kvalifiserte mistanker om at noen har til hensikt å begå alvorlige kriminelle handlinger. *Enklere å overvåke*. Dagsavisen, 12.3.2016

Mass surveillance is unfair because it treats innocent citizens like suspects without any prior evidence of suspiciousness. It therefore undermines the presumption of innocence.

Mass surveillance is inefficient in reducing security threats.

Targeted surveillance is good/better than mass surveillance, because it will only affect suspects/offenders/terrorists.

Targeted surveillance is efficient in preventing security threats.

These assumptions imply that the risks/downsides of mass surveillance can be reduced or eliminated by imposing on those doing the surveillance a requirement for *suspicion*. This will make the surveillance (more) targeted, and hence more acceptable.

An underlying assumption is that it is easy to categorise and/or sort potential offenders from law-abiding citizens.

This framing ignores the fact that both surveillance measures are aimed at detecting potential suspects, not investigate already committed crimes. This makes the distinction innocent citizen/guilty offender even more difficult.

False positives – the “Bycatch”

We need to start talking (more) about false positives and presumption of guilt.

We need to critically scrutinize the potentially positive aspects of mass surveillance.

We need to critically scrutinize the potentially negative aspects of targeted surveillance. We especially need to confront the presumption that targeted surveillance is only aimed at (guilty) suspicious individuals. As Hadjimatheou writes, “There are good reasons to think that both the extent to which surveillance treats people like suspects and the extent to which it stigmatises those it affects increases the *more targeted* the measure of surveillance.”²⁰

We also broaden the frame and talk more about the kind of surveillance that targets categories based on profiling. We need to start worrying less with the most and least targeted forms of surveillance and more with those falling somewhere in between. The current framing of mass and targeted surveillance does not allow for that discussion. Surveillance measures based on profiling that are targeted at suspicious categories, carry high risks of both stigmatisation and discrimination against those they affect. They also inevitably result in a high proportion of false positives.²¹

Redefining surveillance measures – from “surveillance” to “interception”

In 2018, the Ministry of Defence, published a law proposal based on the reports on Digital Border Defence. The new law proposal regulating the military intelligence sector in Norway, abandons the surveillance concept and replaces it with “interception”, or more precisely “Facilitated interception of border crossing electronic communication”²² In the white paper, they write that «Facilitated

²⁰ Katerina Hadjimatheou (2014): «The relative moral risks of untargeted and targeted surveillance». In: *Ethic Theory Moral Prac*, vol 17:187-207, p. 190.

²¹ *Ibid*, p. 201.

²² «Tilrettelagt innhentning av grenseoverskridende elektronisk kommunikasjon». See <https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/>

interception' cannot be characterized as 'surveillance'». However, many of the consultation papers disagreed with this change of concept. The Data Protection Authority wrote that "The government must in their revised law proposal acknowledge that this is surveillance of their citizens and be open about this", and further that "The Norwegian Data Protection Authority is against digital mass surveillance through 'facilitated interception'». Others kept to the concept "surveillance": «Amnesty International is against the proposal to give the Intelligence Service the power to collect and store bulk communication data. Such mass surveillance will be a serious interference in the right to private life and constitute a real danger for the right to free speech and other human rights.» Elektronisk Forpost Norge, a NGO concerned with online privacy, challenged the proposed redefinition in this way: «The white paper proposes that surveillance is not surveillance until the moment when the data are used. Redefining concepts does not cover up the fact that this is technological mass surveillance with the use of military technology»

What we can see from this latest debate is a move away from the former debate on whether a proposed measure is mass or targeted surveillance and towards a debate on whether a proposed measure is surveillance or interception.