Grading advice/Sensorveiledning for KRIM2957 'Surveillance: Data, Technologies, Practices' School Exam

Dear examiners,

Let me start by thanking you all for agreeing to grade exams for this course. KRIM2957 is a BA level elective course that focuses on many of the pressing issues related to surveillance in contemporary societies. The goal of the class is to get students thinking critically about the impact of surveillance in a variety of societal contexts using a range of concepts and frameworks. While the course is popular with criminology students, many students have other academic backgrounds and no prior familiarity with criminology is expected. Given that the course is taught in English, there are also many international students sitting the exam. You will find the exam text below where I have added question specific advice for you **[in brackets]**.

First, here is some general information for you to keep in mind:

The students have **4 hours** to answer **all three questions**: **2 shorter questions (max 500 words each) and 1 longer form essay style question (max 1200 words)**. The weight of each question for the final grade corresponds to the word counts, meaning **that the longer essay accounts for a little more than half the final grade**. Failure to answer one of the questions will almost certainly result in a failing grade.

I have informed the students that examiners will value quality over quantity of words but exceedingly short answers will be considered incomplete and graded accordingly. In concrete terms (which I did not spell out for the students), we should expect approximately 400 word answers for questions 1 and 2, and roughly 1000 words for question 3**. The total word count should be somewhere in the 1750-2200 range**. Anything less than 1750 will have to be of exceptional quality to earn a decent.

As this is a **closed book exam** with no external materials or syllabus provided, there is **no expectation of extensive referencing or reference list**. That said, students are expected to be able to associate key authors to certain concepts and frameworks. Year of publication and page numbers for references are not expected.

Finally, as concerns language quality, I would lean on the side of generosity when it comes to grammatical and spelling mistakes. I don't know what kind of autocorrect function exists on the computers the students are using for their exams, but we can assume that English is not a first language for many students. Be kind, provided of course that there is a discernible meaning to the text. I think that about does it for general advice, but you can always reach out to me if questions arise.

All the best,

Stefano

KRIM2957 BA School Exam

Answer the following 3 questions by drawing on your knowledge of the course content. Questions 1 and 2 are short form questions. Question 3 is a long form question, meaning that you are expected to write a longer and more structured answer that follows an essay structure with an introduction, a main body, and a conclusion. Please note and respect the word limits for all three questions. Good luck!

Question 1: Define and explain the Panoptic model of surveillance. Drawing on your knowledge of the course content, discuss the model's strengths and weaknesses for understanding contemporary forms of surveillance. (Maximum 500 words)

[The Panoptic model of surveillance is the cornerstone of surveillance scholarship. The Panopticon is an architectural design for a prison first proposed by Jeremy Bentham that was made famous by Foucault in Discipline and Punish (1975/1977). If you're not familiar with the model, I suggest a quick google to see it for yourself. Foucault argues that the panopticon is more than just an efficient way to design a prison, but rather the quintessential model of power in disciplinary societies that relies primarily on a strict structuring of enclosed spaces and the asymmetric visibility between the guards in the central tower (who can see all the cells but are not visible from the outside) and the prisoners (who are totally visible to the guards but cannot see inside the central tower nor their neighbours).

Because the prisoners do not know if and when they are being observed, they come to internalize the notion that they are under constant surveillance even if there are no guards on duty. Foucault maintains that this panoptic model can be used in many institutional contexts beyond the prison: the school, the hospital, the factory, the monastery, the military barrack, etc.

Here are some points that we should expect in the answer:

-Panoptic model relies on tightly controlled spatial and temporal conditions and the asymmetric visibility between watcher and watched

-Powerful model for explaining top-down surveillance in a variety of institutional contexts

-Less effective or ineffective for explaining bottom-up surveillance (sousveillance) and lateral/horizontal surveillance

-Linked to disciplinary societies that correspond roughly to the late 18th century to mid-20th century. While there are still disciplinary institutions today, the question is whether we have transitioned to a new dominant model of power defined more by the tracking of flows in open environments, i.e., the society of control as theorized by Deleuze.

-Some applicability to online surveillance, especially the persistence of asymmetric visibility, but there are different spatio-temporal conditions online than in an enclosed building that the panoptic model doesn't fully capture.]

Question 2: What is Big Data and how is it changing the purposes and practices of surveillance? In your answer, discuss relevant concepts from the course content as well as relevant empirical examples. (Maximum 500 words)

[Big Data is broadly defined as the analysis of massive amounts of data pooled from different sources (police records, insurance records, medical records, consumer profiles, etc.) to uncover useful but not obvious patterns. Big Data is often associated with three "Vs": volume, variety, and velocity. The sheer amount of data is too great for any human individual or group to handle, requiring the use of algorithmic software. Some of these algorithms are rule-based (parameters are set by developers), but many are increasingly machine-learning based (parameters can be revised by the software itself), meaning that even the developers don't even know how their software systems arrive at their findings.

Big Data changes the purpose of surveillance from identification and record-keeping to prediction and behavioural modification. The goal is not perfect accuracy, but rather utility for decision-making. Rather than trying to find predefined targets, big data gives states and companies the capacity to democratize surveillance to all individuals to anticipate threats and push products as quickly and early as possible.

Here are additional points I would expect (in some combination):

-Big data is linked to the concepts of "surveillance capitalism" (Zuboff) and the "surveillant assemblage" (Haggerty and Ericson).

-Surveillance capitalism is about the use of big data and consumer profiles to shape consumption patterns for individuals.

-Haggerty and Ericson's concept of the surveillant assemblage was proposed in 2000 and anticipated many of the developments now associated with big data. They argued that there was a centralizing tendency to surveillance practices whereby datasets would be networked and combined to create "data doubles" of individuals that could inform policy, policing and business decisions.

-Big data can launder biases that exist in datasets as is for predictive policing software that uses racially-biased policing data to anticipate crime and allocate law enforcement resources. Big data gives these biases the veneer of objectivity and impartiality.

-The velocity of big data systems is meant to provide real-time information, important for tracking tasks and flow management

-The lack of transparency (the fact that big data software is a 'black-box' even to its developers) challenges democratic decision-making processes.

-Unethically sourced data concerns

-Possible empirical contexts: predictive policing, government surveillance (Palantir), tech giants (Google, Amazon, Meta) and other commercial interests, GPS services like google maps, financial systems]

Question 3: Read and analyze the article below. In your essay, select and use two concepts or perspectives from the course content that you think best explain the trends in surveillance relevant to the article. (Maximum 1200 words)

[Read the article below. This question is very open-ended so there aren't any "correct" answers per se. The students will probably lean on whatever concepts/perspectives they have prepared the most and that's quite alright. As a result, grading will rely more on the level of critical thinking and analytical nuance on display. Points should also be awarded/deducted for structure or lack thereof. The exam text at the top clearly states that we expect an essay structure with introduction, main body and conclusion.

Here are some potential pathways students might take:

-Computerized workplace surveillance is increasingly important as hybrid work arrangements become more common. This forces surveillance practices to adapt and become less bound to physical workplaces, and thus less panoptic in a certain sense.

-Big data and AI angle: AI is being used to monitor behaviour, but it is interesting that employees express concern that the goal could be to train AI to replace them.

-Biometric surveillance angle

-Resistance to surveillance: the article is generally critical of these trends as are many of the sources quoted in the piece. The article and its sources point to discontent and resistance to increased surveillance. Nuanced responses would discuss exactly how effective/viable that resistance can be, especially in the workplace.

-Societies of control v disciplinary societies, a more theoretical angle that discusses the shift from surveillance and discipline in enclosed spaces, to tracking and modulation in open environments.

These are just some of the angles that come to my mind, but again, the students are free to take this in any direction they see fit, provided that it is relevant to the article.]

Article Title: A third of UK firms using 'bossware' to monitor workers' activity, survey reveals

Author, Date and Outlet: by Robert Booth in The Guardian, published September 14 2025

Article text: A third of UK employers are using "bossware" technology to track workers' activity with the most common methods including monitoring emails and web browsing.

Private companies are most likely to deploy in-work surveillance and one in seven employers are recording or reviewing screen activity, according to a UK-wide survey that estimates the extent of office snooping.

The findings, shared with the Guardian by the Chartered Management Institute (CMI), are based on responses from hundreds of UK managers and suggest there has been a recent growth in computerised work surveillance.

In 2023, less than a fifth of people thought they were being monitored by an employer, the Information Commissioner's Office (ICO) found. The finding that about a third of managers report their organisations are monitoring workers' online activities on employer-owned devices is probably an underestimate, as roughly the same proportion said they don't know what tracking their organisations do.

Many monitoring systems are aimed at preventing insider threats and safeguarding sensitive information as well as detecting productivity dips. But the trend appears to be causing unease.

A large minority of managers are opposed to the practice, saying it undermines trust with staff and invades their personal privacy, the CMI found.

One manager at an insurance company, which is developing AI systems to monitor staff screen activity to track performance, said it was “unsettling”.

“Do they not trust their employees to do their jobs and are they looking to replace them with AI?” they said.

One provider of employee monitoring offers to report on workers’ “idle time”, “employee productivity tracking” and use of unapproved AI or social media as well as “real-time insights into employee behaviour, including screenshots, screen recordings, keystrokes, and app usage”.

In response to the findings, the ICO said bosses “must make their employees aware of the nature, extent and reasons for monitoring”, and said excessive monitoring “can undermine people’s privacy especially if they are working from home”. It warned it will “take action if necessary”.

Last year, the ICO stopped the outsourcing company Serco from using facial recognition technology and fingerprint scanning to monitor the attendance of staff at a chain of leisure centres.

Monitoring often amounts to checks that inappropriate content is not being accessed, the CMI said. But it warned, “there’s a longer-term impact if you are feeling this is big brother-like and you are being watched”.

“If it is being used, it is incredibly important employers are open, otherwise that’s going to cause significant problems in terms of data privacy and protection,” said Petra Wilton, CMI director of policy and external affairs.

Other recent examples of surveillance technology at work include plans by HSBC to install a large numbers of security cameras – 1,754 by one estimate – and biometric readers which use handprints as one way to access areas in its new London headquarters.

The accountancy firm PwC recently introduced a “traffic light” system using data from pass swipes and wifi connections to check staff are meeting a mandate to attend the office at least three days a week. A spokesperson for PwC said this was “accepted by the vast majority of our people”.

A former senior worker at a public transport authority, who asked not to be named, called the monitoring they faced, including of their online diary, “intrusive and downright harassment”.

“It started with surveillance and it ended with me leaving because I was so infuriated,” they said. One in six managers also told the CMI researchers they would consider looking for a new job if their organisation started monitoring employees’ online activities on work devices.

Among managers who knew their organisations carried out surveillance, 35% were monitoring emails. Overall, tracking log in and log off times and system access were the most popular form of surveillance.

The study found that 53% of managers supported monitoring of employees’ online activities on employer-owned devices, but 42% opposed it, mostly because it undermines trust but also

because they believe it does not improve performance and can be misused or lead to unfair judgments or disciplinary actions.