The Economics of Surveillance

Carly Beckerman* and Julian Williams

Synonyms

Monitoring; Corporations; Security; Privacy; Political Economy;

Definitions

Surveillance is the action by an individual or organization to collect information on the activities, actions and statements of another individual or group. The origin of the word surveillance is rooted in the portmanteau of the french words for 'over' (sur) and 'watch' (veillier). As such, a modern interpretation of 'mass surveillance' refers to watching the activities of large groups, usually through a variety of methods associated with electronic devices, from cellular communications to internet-based mechanisms. Although surveillance is not new, the economics of surveillance and the justification of surveillance from a social coordination perspective are relatively recent additions to the canons of information economics and public economics. These sub-fields discuss the rationale for legal limits on surveillance and arguments in favour of protecting privacy, as well as the cost-benefit analysis that policy-makers conduct to determine optimal degrees of surveillance for social welfare. There is an inherent appreciation within these debates that the economics of surveillance reflects a trade-off between control and well-being. Rule, for example, defines the surveillance domain of interest as:

> *"...any systematic attention to a person's life aimed at exerting influence over it. By social control we mean efforts to define and bring about "correct" actions or statuses."*

(Rule et al 1983, Page 223.2).

Although the legal and social implications of mass surveillance for public

* corresponding author

control have been reviewed extensively from a constitutional law perspective, (see, for example, Rackow (2002) for a reaction to the Patriot Act and Kerr (2008) as a response to the Foreign Intelligence Surveillance Act (FISA) in the United States), economic models of the political economy of mass surveillance are quite sparse.

Theory

Information economics provides the basic motivation for surveillance. Let $a_i \in \mathscr{A}_i$ be a set of continuous actions for a discrete agent indexed by $i \in \{1,\dots,I\}$ and let $V_i(a_i, \boldsymbol{a}_{-i})$ be a value function that sets out the payoff for agent i, given their action a_i with respect to the actions of all other agents $\boldsymbol{a}_{-i}$. In a classic utilitarian set up, the social planner observes a payoff of $U_P = \sum_{i=1} w_i V_i(a_i, \boldsymbol{a}_{-i})$. In the simplest setting, an agent i constructs a statistical model of all other agents. The degree of precision in this model reduces the uncertainty in the payoff $V_i(a_i, \boldsymbol{a}_{-i})$. A simple setting has a Von Neumann–Morgenstern expected utility function of the form $U^e = \mathbb{E}_i[V_i(a_i, \boldsymbol{a}_{-i})|\mathbb{E}[\boldsymbol{a}_{-i})] - \gamma \text{Var}[V_i(a_i, \boldsymbol{a}_{-i})|\text{Var}[\boldsymbol{a}_{-i})]$. For any given degree of aversion to variance, the utility for a higher precision (hence the lower variance of $\text{Var}[\boldsymbol{a}_{-i})$ as the only contribution to the variance $\text{Var}[V_i(a_i, \boldsymbol{a}_{-i})|\text{Var}[\boldsymbol{a}_{-i})]$) is via uncertainty in the other players actions. From a classical economic perspective, any cost of information from surveillance is weighed against the benefits to the reduction in uncertainty and the ability to gain new levels of expected utility. Denote the expected and variance of the payoff with surveillance as $\mathbb{E}_i[V_i(a_i, \boldsymbol{a}_{-i})|\mathbb{E}[\boldsymbol{a}_{-i}); c]$ and $\text{Var}[V_i(a_i, \boldsymbol{a}_{-i})|\text{Var}[\boldsymbol{a}_{-i}); c]$. For many applications of surveillance, the following pair of inequalities holds true:

$$\begin{aligned} &\mathbb{E}_i[V_i(a_i, \boldsymbol{a}_{-i})|\mathbb{E}[\boldsymbol{a}_{-i}); c] \\ &\qquad > \mathbb{E}_i[V_i(a_i, \boldsymbol{a}_{-i})|\mathbb{E}[\boldsymbol{a}_{-i})] \qquad (1) \\ &\text{Var}[V_i(a_i, \boldsymbol{a}_{-i})|\text{Var}[\boldsymbol{a}_{-i}); c] \\ &\qquad < \text{Var}[V_i(a_i, \boldsymbol{a}_{-i})|\text{Var}[\boldsymbol{a}_{-i})]. \qquad (2) \end{aligned}$$

Therefore, expected gains from information gathering exhibit first order stochastic dominance. The neoclassical economic view of information asymmetry and the gains from information acquisition are reviewed, qualitatively, in Löfgren et al (2002), Cohen (2010) and later Cohen (2018), amongst others.

This approach, however, is too simplistic and only applicable to cases such as sports teams spying on opponents, corporate espionage, and massive data gathering by firms hoping to extract greater surpluses from their consumers. Unfortunately, without more specific assumptions regarding the externalities of mass surveillance, social welfare implications remain somewhat opaque from a public economics perspective.

Network models may offer a useful approach to the production of public goods through adjoint interactions, with measures of closeness within the node structure acting as a proxy for the spillovers between individual agents. Danezis and Wittneben (2006), for example, utilizes a stylized network structure to illustrate quantitatively the returns to large scale network surveillance on actions. The social planner may then monitor these interactions and make interventions based on a series of policy rules. In the case of benevolent planning, this procedure is

designed to increase security and reduce externalities. In the less benign case, surveillance is used to extract surpluses from the population and increase political power and financial reward for the planner. Unfortunately, as of writing, there are no fully realized network based economic models with explicit reference to surveillance. However, as the theoretical tools for network economics develop, applied models with an explicit quantitative treatment of surveillance will surely follow.

In contrast to the quantitative treatments, qualitative research on surveillance is manifold. Boghosian (2013) and Zuboff (2019) provide commentaries on corporate mass surveillance, with the latter discussing a framework for "surveillance capitalism" as a general construct. The concepts in Zuboff (2019) are further elaborated in Cuellar and Huq (2020), which identifies a series of economies tied to technologies such as big data processing, machine learning and other aspects of artificial intelligence. These technologies incentivize mass surveillance for commercial gain.

The commercial incentive to acquire information from mass surveillance is reasonably well understood when theorizing from the firm's perspective. However, a number of complicating factors can obscure governmental incentives for pursuing mass surveillance.

Conventional economic tools, for example, do not adequately describe why governments invest substantial financial and reputational capital in electronically monitoring their own citizens. This is surveillance in addition to traditional intelligence gathering that aims to detect security threats. In this instance, there appear to be number of trade-offs that determine the optimal investment by government in mass surveillance.

First is the notion of the collective safety and security of citizens as a public good versus the right of the individual to have ownership of a private sphere. Second is the government's desire to provide optimal delivery of public services versus the ruling classes' ability to maintain their power and extract surpluses through rewards and punishments determined by mass surveillance. Finally, there are cross interactions between these two trade-offs.

Concerns over the centralization and preservation of power are outlined in Walton (2001) with an early analysis of the Chinese government's approach to information management within the context of the burgeoning internet. In a cursory review, Ball and Wood (2013) comments on the key notions of why political decision makers value information collection and how this clashes with reasonable expectations of privacy. With reference to the simultaneous British and American revelations on mass surveillance programs, Stahl (2016) discusses the implications for political power, privacy and the public sphere.

Nevertheless, while concerns regarding power, persuasion and security are well developed, there are no true theoretical models that determine the need for comprehensive mass surveillance by government. A simple model that captures this effect is a bundle $r \in \mathscr{R}$ where $r = \{p, s, g\}$, where $\mathscr{R}$ is a feasible set determined by technology. Citizens gain welfare from indexed quantities of privacy p, security s, and consumption g. For some utility function $\mathscr{U}(r)$, such that $\mathscr{U} : \mathbb{R}^3 \to \mathbb{R}$, we can write down sequences of preferences between tuples of $\{p, s, g\}$. Hence, we

can predict from revealed preferences the shape of the psychological trade-off between individual components. There are implied cross partial derivatives of $\mathscr{U}(r)$ that are recovered from sequential analysis of preferences for pairs of bundles. For instance $\mathscr{U}(r_a) > \mathscr{U}(r_b)$, means that r_a is strictly preferred to r_b or $r_a \succ r_b$ with varying quantities of p, s and g. By constructing lattices of many pairs and determining the strict order of preferences by systematically varying, p, s and g the implied tolerance of surveillance can be determined by the trade-off between the optimal levels of p and s for given levels of g.

The optimal bundle r^*, under a utilitarian social planner, is the Pareto efficient quantities of privacy, security and consumption. Goh (2015) describes one solution to this problem by assuming a representative citizen with a particular functional form for security and consumption preferences. Planning problems may also be less benign. For instance, in a kleptocracy, the dictator chooses a tuple $r^\dagger$ that maximizes their subjective utility, and this is subject to the constraints of ensuring their power base from domestic and foreign threats. Indeed, even when extending the utilitarian social planner approach to multiple public domains, it is possible to observe perfectly rational models of intrusive surveillance. Consider a case in which the social planner is utilitarian with an aggregated social welfare function $U_P = \sum_n U_n(r_n)$. Aggregate utility is in respect to a domestic public, indexed by $n \in \{1,\ldots,N\}$. However, the planner has no specific utilitarian benevolence towards a second foreign public indexed by $m \in \{1,\ldots,M\}$. If surveillance of the overseas public allows the domestic public to generate direct positive returns with minimal cost, then a corner solution could be achieved where p_m effectively tends to some lower bound usually decided by technical feasibility, whilst p_n is maintained at some specific optima. In this case even small gains to s_n achieved by an aggressive reduction in p_m would be justifiable.

However, tolerance to perceived surveillance may not involve quantities of privacy. Any cost benefit analysis associated with mass surveillance is additionally complicated by the apparent effectiveness of implicit observability cues. If, per Rule et al (1983), the aim is to foster "correct" or pro-social behaviours, then merely creating the sense that people might be observed (through, for example, posters featuring instructions to the public and images of large eyes trained on the viewer) is enough to encourage otherwise costly behaviours such as vote participation. See, for example, Haley and Fessler (2005) and Panagopoulos (2014). In an ironic juxtaposition, Backer (2004) notes that the regulatory surveillance panopticon that was envisioned under Sarbanes–Oxley to promote pro-social corporate behaviour has met fierce resistance among the corporate officers subject to such surveillance. A further extension in Backer (2008) describes the 'unbundling' of surveillance into these different modes, most notably passive and active approaches to monitoring. Comparing corporate surveillance and the wider set of surveillance tools used by government Backer (2008) examines, from a legal perspective, the power dynamics associated with varying bundles of privacy, security and consumption.

Whilst the effects of surveillance across modes is likely to be pervasive, the ordering of the preferred bundles is

unlikely to be persistent across contexts. For example, after terrorist attacks and pandemics, the cross products that define the trade-offs between privacy and security may change substantially. A population's experience of negative events re-weights the trade-off between privacy and security for a particular growth contour. Particularly in the case of re-weighting due to security crises, it can also be difficult for policymakers to anticipate the trade-offs accurately. In the UK, for example, surveillance measures included in the counterterrorism strategy 'Prevent' disrupted many British Muslims' sense of citizenship, creating a new layer of alienation that nourished rather than stemmed radicalisation. See, for example, Blackwood et al (2016). Likewise, Edney-Browne (2019) notes how American drone surveillance in Afghanistan has caused social isolation and self-objectification among ordinary people who feared that their community gatherings and celebrations would be targeted from above as suspicious. Although this drone surveillance has had immediate military benefits, the psychological impact on ordinary Afghans has also been counterproductive for American security goals in the region.

Open problems and Future directions

Despite the extensive evaluation of the socio-political notions of surveillance, a fully realized theoretical model of mass surveillance with specific reference to the digital economy is still elusive. While Danezis and Wittneben (2006) provide one of the few fully worked models, the degree of simplicity and the lack of an appropriate analytical deconstruction makes this an unsatisfactory touchstone for the political economy of mass surveillance. Another approach is to model the growth structure of an economy with surveillance directly, as in Goh (2015). The value of monitoring to both agents varies across the range of the surveillance set that government engages in. One prediction from the model is that incompetent leaders tend to entrench themselves by engaging in excess surveillance, a neat prediction that holds up against empirical evidence.

Finally, as noted above, the blanket assumption that surveillance increases security has been widely challenged implicitly and explicitly. See Davis et al (2014), for example. Of particular concern moving forward is the political "backdooring" of economically important information systems. The surveillance of private communications through messaging and electronic mail reduces societal security and increases individual costs by delivering proofs of concept to criminal actors. Conceptually, we know that criminal actors tend to target vulnerabilities in software that have well understood weaknesses. The pay-off from researching and developing an exploit that ex-filtrates data needs to be achievable in a finite time, with a reasonable cost compared to gain. A state actor has no specific need to return a revenue from their surveillance efforts (although the secondary revenue may be high from maintaining power structures), but researching a proof-of-concept for the existence of a feasible exploit acts as a bounty to actors with finite resources. Indeed, any public disclosure of the exploit further reduces costs for a wide range of non-benign

actors who would not otherwise be incentivized to build such tools. In this sense, the existence of intrusive surveillance designed to subvert the integrity of private information ultimately creates more direct costs to the planner and negative externalities across society.

Cross-References

Privacy Economics, Privacy in social networks, Privacy laws and directives.

References

Backer LC (2004) Surveillance and control: Privatizing and nationalizing corporate monitoring after sarbanes-oxley. Mich St L Rev p 327

Backer LC (2008) Global panopticism: states, corporations, and the governance effects of monitoring regimes. Indiana Journal of Global Legal Studies 15(1):101–148

Ball KS, Wood DM (2013) Political economies of surveillance. Surveillance & society 11(1/2):1–3

Blackwood L, Hopkins N, Reicher S (2016) From theorizing radicalization to surveillance practices: Muslims in the cross hairs of scrutiny. Political Psychology 37(5):597–612

Boghosian H (2013) Spying on democracy: Government surveillance, corporate power and public resistance. City Lights Publishers

Cohen E (2010) Mass surveillance and state control: the total information awareness project. Springer

Cohen JE (2018) The biopolitical public domain: The legal construction of the surveillance economy. Philosophy & Technology 31(2):213–233

Cuellar MF, Huq AZ (2020) Economies of surveillance. Harvard Law Review 133(4):1280

Danezis G, Wittneben B (2006) The economics of mass surveillance. In: Fifth Workshop on the Economics of Information Security

Davis T, Peha JM, Burger EW, Camp LJ, Lubar D (2014) Risking it all: Unlocking the backdoor to the nation's cybersecurity. Available at SSRN 2468604

Edney-Browne A (2019) The psychosocial effects of drone violence: Social isolation, self-objectification, and depoliticization. Political Psychology 40(6):1341–1356

Goh B (2015) Prosperity and security: A political economy model of internet surveillance

Haley KJ, Fessler DM (2005) Nobody's watching?: Subtle cues affect generosity in an anonymous economic game. Evolution and Human behavior 26(3):245–256

Kerr OS (2008) Updating the foreign intelligence surveillance act. The University of Chicago Law Review 75(1):225–243

Löfgren KG, Persson T, Weibull JW (2002) Markets with asymmetric information: the contributions of george akerlof, michael spence and joseph stiglitz. The Scandinavian Journal of Economics 104(2):195–211

Panagopoulos C (2014) I've got my eyes on you: Implicit social-pressure cues and prosocial behavior. Political Psychology 35(1):23–33

Rackow SH (2002) How the usa patriot act will permit governmental infringement upon the privacy of americans in the name of" intelligence" investigations. University of Pennsylvania Law Review 150(5):1651–1696

Rule JB, McAdam D, Stearns L, Uglow D (1983) Documentary identification and mass surveillance in the united states. Social Problems 31(2):222–234

Stahl T (2016) Indiscriminate mass surveillance and the public sphere. Ethics and Information Technology 18(1):33–39

Walton G (2001) China's Golden Shield: corporations and the development of surveillance technology in the People's Republic of China. Rights & Democracy

Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019. Profile Books