

# Can Privacy be the antidote to Mass Surveillance?

By Pablo Ouziel

***Abstract:** When I think of the term mass surveillance, I often wonder, whether victims of the Holocaust would have been comfortable providing their personal information to governments and organizations, if they had known, that later this information would be used for the social profiling which destroyed their lives. Much time has passed since these events that marked the second half of the 20<sup>th</sup> Century, and are still marking the early stages of the 21<sup>st</sup>. Today, technological advancements, supporting legislation, political and corporate will, and the acceptance by a majority of the population, have allowed the spread of surveillance methods and tools, which are far more sophisticated and effective than those used all those years ago, to round up the victims of the Holocaust. This statement sheds light on a worrisome fact: While most Western industrialized democratic societies have focused on growth, efficiency, comfort and perceived security. There exists a possibility, that this very drive has exposed these populations to unnecessary potential threats of worrisome magnitudes. It is these unnecessary potential threats, which have led many intellectuals and activists towards developing an effective antidote to mass surveillance; numerous Privacy rights advocates, deem their cause as the most effective antidote. Yet, pointing to the volume and function creep we have experienced in the realm of mass surveillance, others claim privacy has not worked. This article aims to determine whether privacy can indeed be the antidote to mass surveillance.*

## Counteracting Mass Surveillance

Kevin Haggerty and Richard Ericson have rightly pointed to the risk of surveillance as an analytical category being stretched beyond all recognition (Haggerty and Ericson 2006, 21). For this reason, since this article addresses the question of whether privacy can serve as an antidote to mass surveillance, prior to discussing privacy, it is important to describe what mass surveillance is, in order to keep it within recognizable analytical confines.

A recent House of Lords report on *Surveillance: Citizens and the State*, has identified two broad forms of surveillance: mass surveillance and targeted surveillance (House of Lords, Constitution Committee - Second Report. *Surveillance: Citizens and the State*, Session 2008-09). Amongst academics studying mass surveillance, there seems to be wide spread consensus, describing mass surveillance as pervasive surveillance on a large proportion of a particular population. Although traditionally, mass surveillance has been considered to be an attribute of totalitarian states, in today's Western industrialised democratic societies, both corporations and the state conduct mass surveillance – and frequently the information collected is shared between the two.

James Rule (2007, 21) speaks of systems of mass surveillance, as systems, which have no natural limit to the incorporation of personal information. Gary Marx, claims these systems shift the ratio of what individuals know about themselves versus what outsiders and experts can know about them, away from the individual (Marx 1999, 40). Felix Stalder has contributed to Marx's point, by emphasizing that while 'they' know more than ever about 'us', we still know very little about 'them' (Stalder 2002, 121). From Stadler's statement, one can deduce that mass surveillance societies are operating most effectively, when individual citizens provide increasing amounts of information, without being able to determine who is benefiting from the data being collected.

Despite the fact that there is a clear separation between those who collect information and those who provide it, there is at present a social acceptance to mass surveillance. Michael Curry seems to attribute this acceptance, to a lack of understanding regarding the digital

individuals (data-doubles) which are proliferating in our modern information societies: “Once we begin to understand that these individuals – carrying our names, addresses, and social security numbers – are talking for us, representing us, and making decisions for us, we can see that they are very much like the fragmented parts of ourselves that we present in every part of our everyday life” (Curry 1997, 695). Curry seems hopeful, that once social awareness around this issue grows, just as the majority of the population feels we have control over our actions in everyday physical life, society will soon realize the importance of having “control over that much wider range of virtual selves, to the creation of which we have been only partially willing collaborators” (Curry 1997, 695).

Perhaps Curry is right, and in the future we can expect a reversal of the social acceptance to mass surveillance. However, in the meantime, what we are witnessing in most Western industrialized democratic societies is an ever growing electronic connectivity, which functions by extracting huge amounts of personal data, which is processed, manipulated, traded and used to influence and direct individual and collective action. These events, have led David Lyon to conclude that the surveillance society is the obverse of the information society (Lyon 2001, 108). Supporting this view, Tony McNulty – MP and former Minister for Security, Counter-terrorism, Crime and Policing at the Home Office in the UK – acknowledges that surveillance tools such as CCTV, DNA databases and a whole range other elements have become routine in the 21<sup>st</sup> century (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09).

In view of this routine use of mass surveillance, it is important for society to pay attention to the worrisome aspects of such practice. What follows, are a few reasons why mass surveillance poses concern: *First*, the fact that the ultimate aim of mass surveillance systems is to discriminate, for they seek to determine warranted actions toward individual members of large populations (Rule 2007, 15). *Second*, the danger highlighted by NO2ID – the UK advocacy group opposing identity cards – which claims that growing emphasis on records and centralised databases, undermines the presumption of innocence, by making anyone who is not willing to provide requested information a target of suspicion (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09). *Third*, the acknowledgment of a function and volume creep inherently adopted by existing systems of mass surveillance, and *fourth*, the realization that accessing large data sets of personal information provided by mass surveillance mechanisms, is a prerequisite for social control. It is these points, which warn us of the need to understand mass surveillance and its outcomes and possible consequences, in order to challenge its spread through fresh and effective methods.

### **Privacy as the antidote to Mass Surveillance**

Repeatedly, academics studying surveillance have voiced concerns about the difficulty of removing surveillance mechanisms once they have been put into operation. Frequently, because of the benefits that they offer, as citizens we are driven into legally, politically and culturally accepting new forms of surveillance. Nevertheless, as a recent statement by Vernon Coaker – MP and former Minister for Drugs & Crime Reduction – clearly demonstrates, on many occasions we are misguided into consent. In justifying the need

for state surveillance, Coaker argues that “society should respond in the appropriate way to the threat that it faces at that particular time, always having regard to the need to balance national security with human rights” (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09). This statement, which on the surface might seem reasonable, when analyzed in detail reveals its inaccuracy. National security should never be balanced with human rights, national security should serve for the purpose of defending human rights at all times. Awareness of this by civil liberties groups, human rights activists, privacy activists and academics in numerous fields, has encouraged a search for the right antidote against surveillance; through this search, privacy has been hailed by many as the answer to the surveillance question. Yet, although on occasions it has been reasonably effective as the antidote for targeted surveillance, it is still in the embryonic stages of becoming a full-fledged antidote to mass surveillance.

A whole century has passed since Samuel Warren and Louis Brandeis wrote their legendary paper on *The Right to Privacy*. Even so, on a 1990 article on privacy and gender, Anita Allen and Erin Mack accused Warren and Brandeis of being patriarchic and elitist, and rejected their place in history as privacy revolutionaries (Allen and Mack 1990, 466). Although I agree with parts of the argument made by Allen and Mack, I feel that Warren and Brandeis must be acknowledged as founders of the modern privacy movement, for despite their elitist goals, through their defence of the right to privacy, they carved a way for the protection of individuals against surveillance. Today, however, in the same way that surveillance has flourished and evolved, privacy advocacy needs to

transcend its inherently personal definition of privacy and work towards defining it as a collective right, instead of reusing it as a patriarchal and elitist value. As Stadler has pointed out, the 19<sup>th</sup> century conceptual framework of privacy does not apply to the 21<sup>st</sup> century (Stalder 2002, 122). Since the 19<sup>th</sup> century, in most Western industrialized democratic societies, individuals have shifted from being relatively un-scrutinized by private organizations and government agencies, to being routinely monitored by them. For this reason, if privacy is to be the appropriate antidote to mass surveillance, privacy advocacy must evolve.

Since the days of Warren and Brandeis the right to privacy has become the dominant legal and public discourse to forestall the encroachment of surveillance. Nevertheless, because of its diffused and holistic nature, advocates of the value of privacy have found it difficult to stop the spread of surveillance. In fact, many academics and activists have begun to voice the concern, that in many instances data protection and privacy regulation “has apparently inoculated surveillance institutions against public indignation” (Rule 2007, 32). This concern, has consequently led many critics of privacy advocacy towards the argument made by David Lyon, that failures of privacy to stop surveillance, are due to the fact that privacy language is “still part of the hegemonic system of consent to the dominant liberal culture of law and the establishment” (Lyon 2001, 137).

Acknowledging this stance, although I do not disagree with Lyon, rather than seeing privacy’s involvement in the hegemonic system of consent as the sole reason for its failure to obstruct surveillance, I see a myriad of obstacles that have reduced the strength

of privacy as an antidote to surveillance. *First*, the fact that privacy protection has not often addresses the most pressing question: “What purposes, what interests warrant creating and maintaining surveillance systems?” (Rule 2007, 24). *Second*, the reality that although many public opinion studies have reflected social concern about losses of privacy, these have not frequently translated into social demands for legislation defending privacy rights. *Third*, the observation, that in most contestations over privacy, individuals or small civil liberties groups, are up against well-funded institutions. *Fourth*, the realization, that privacy rights are being reconfigured to defend corporate and state interests. *Fifth*, the undeniable reality, that resistance to surveillance is typically motivated by a desire to evade personal scrutiny and not to dismantle existing surveillance systems. *Sixth*, the acknowledgment that in most Western industrialized democratic societies, we are witnessing the “‘ratcheting down’ of officially defined ‘reasonable expectations of privacy’” (Rule 2007, 161). *Seventh*, the fact that “privacy advocates have hurt their cause by acquiescing to, or even promoting, notions that privacy is somehow compatible with relentless efficiency maximization in government and private institutions” (Rule 2007, 192). And *eighth*, the fatalism, which leads many to assume, that there is no room for privacy in a society that strives to total surveillance – this last point, being the one, which neutralises the privacy antidote against mass surveillance.

While I consider myself a critic of privacy advocacy for its lack of effectiveness, and I encourage privacy advocates to seriously consider the points stated above; I also acknowledge the fact that privacy language is an existing language, and it would be a

mistake to eradicate it. Despite its limitations, I am convinced that privacy language and action aimed at defending privacy rights are the most effective antidotes to targeted surveillance. I am also confident that if reconfigured properly, privacy can also become an effective antidote to mass surveillance. In order for this to happen, we must take the concept of privacy and adapt it to current social conditions, acknowledging mass surveillance as one of the biggest threats to our human rights and collective privacy. Recently, the Trustguide project conducted a focus group research in the UK, which revealed “we are at a tipping point of public acceptability of surveillance and data collection” (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09). Perhaps this observation will transform into action, and privacy advocacy will acquire the critical mass necessary to defend the privacy cause.

From a broader perspective, it is important to note, that although mass surveillance affects a very large number of people, it does so in very small ways – this makes it very difficult to single out a particular victim or identify a single serious harm. For this reason, the way to protect our societies from mass surveillance is to see privacy as a collective value and right, build solidarity and trust in our societies, and keep alive the historical memory, which can remind us of past outcomes of mass surveillance practices. It is clear that the law alone cannot prevent the abuses of those in control of mass surveillance. Mass surveillance practices that are perfectly legal “may nonetheless be undesirable according to other broader ethical or constitutional criteria” (House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session

2008-09). It is these broader criteria, which must be promptly addressed. It is not privacy, which has failed as an antidote to mass surveillance, but the lack of collective will to reverse the growth and spread of surveillance assemblages.

## **Conclusion**

Mass surveillance has two sides; on the one side, it apparently offers speed, security, and safety; on the other, it unnecessarily exposes individuals to potential threats of worrisome magnitudes. Consequently, because of its perceived benefits, the worrisome aspects are usually overlooked. This perhaps sheds light on why resistance is often lacking or simply fails. Conversely, it is important in the early stages of the 21<sup>st</sup> century, for citizens to collectively ask whether the negative aspects of mass surveillance are likely to be mitigated or eliminated if present trends continue? (Lyon 2001, 128). If as academics, activists or concerned citizens, we feel the negative aspects of mass surveillance will not be mitigated if we continue on the current path; then we must move collectively away from trying to maintain an ever-weakening illusion of privacy, and shift to the offensive, by demanding accountability of those whose power is enhanced by mass surveillance (Stalder 2002, 123).

James Rule seems optimistic that we will not head towards a world of total surveillance because nobody wants to live there. Perhaps he is right, as I believe he is, when he acknowledges that the choice of privacy as an antidote to mass surveillance is not an easy one, because “it is not easy to opt for a messier, less efficient, more dangerous and unpredictable world as the price of authentic privacy (Rule 2007, 201). Nevertheless, if

despite this realization, we acknowledge Gary Marx's advice, when he reminds us of the fact, that just like nightfall, oppression doesn't come at once, it passes through a twilight face in which everything is seemingly unchanged (Marx 1999, 63); and we are able to keep our historical memory alive, in order to remember the potential threats of mass surveillance. Then we might come to realize, that current mass surveillance trends must be reversed, and that privacy is the most advanced antidote for the task at hand. Aware of its imperfections, we must make privacy work.

To this end, if we are to understand how to make privacy work as the antidote to mass surveillance, we must *first* keep embodied personhood central to surveillance theory (Lyon 2001, 124). Keeping personhood central, allows us to understand that the only way to protect ourselves from mass surveillance is through collective action. As Marx has pointed out, at an abstract level, there are shared expectations in most Western industrialized democratic societies, whose violation underlines the discomfort experienced in the face of new surveillance practices (Marx 1999, 42). This collective discomfort should inspire the way towards seeing privacy as a collective value, build solidarity and trust in our societies, and keep alive the historical memory, which can remind us of past outcomes of mass surveillance practices. The *second* and most important point, which must be addressed in order to strengthen privacy as an antidote to mass surveillance, is for privacy advocates to adopt a more firm position. Advocates must request that no one suffer the burden of mass surveillance unless there has been previous social debate, and a societal referendum, which together determine that a given practice is warranted and genuinely accepted by the majority of the population. If we are able to

acknowledge the worrisome aspects of Mass surveillance, and we are able to reverse the limitations of privacy by adapting it to the 21<sup>st</sup> century, then perhaps the antidote will work. Until we truly try, we cannot blame it for society's ills.

## **Bibliography**

Allen, A.L. and Mack, E. (1990) 'How Privacy Got Its Gender' in *Northern Illinois University Law Review*, 10: 441-78.

Curry, M.R. (1997) 'The Digital Individual and the Private Realm' in *Annals of the Association of American Geographers*, 87(4), pp. 681-699.

Haggerty, K.D. and Ericson, R.V. eds. (2006), *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

House of Lords, Constitution Committee - Second Report. Surveillance: Citizens and the State, Session 2008-09, available online at:  
<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm>

Lyon, D. (2001) *Surveillance Society: Monitoring everyday life*, Philadelphia; Open University Press.

Marx, G.T. (1999) 'Ethics for the new surveillance', in *Visions of Privacy: Policy Choices for a Digital Age*, edited by Colin J. Bennett and Rebecca Grant, Toronto, University of Toronto Press.

Stalder, F. (2002) 'Privacy is not the antidote to surveillance' in *Surveillance & Society* 1(1): 120-124

Rule, J.B. (2007) *Privacy in Peril*, Oxford; Oxford University Press.