**Heroic Leaks of Information: Quixotic or Practical?**

*Mats Ekman*

This essay makes an economic case for regarding the leaking of information on one's own government's wrongdoings as acts of heroism rather than treason. Just like ordinary property rights tend to be best managed by those who can most easily control the property to which they refer, ownership of personal information is generally best left with the individual to whom the information refers. This individual suffers the consequences if he handles his property badly (e.g., by sharing it with the wrong person), and therefore has an incentive not to do so. This incentive is not as strong under alternative arrangements in which one's personal information is controlled by someone else, particularly if that party faces no competitive pressure to manage it well. Letting it be known that states appropriate vast amounts of personal information can only help citizens better manage their property, which is why information leaks like Edward Snowden are heroes. However, in light of the remarkable improvements in information technology and decline in the price of storing and retrieving information, states, by the Law of Demand, will spy on their citizens in spite of recurrent leaks. This is due to the usual collective action problems studied by public-choice economists. Whether information leaks will impact policy – and whether the leaks are heroes of the quixotic or "practical" kind – therefore depends on institutional features of the invigilating state.

**I - Introduction**

Given the remarkable and continued decline in the price, and the increase in the capacity, of storing and of retrieving information, it is an unavoidable consequence of the Law of Demand that the state will want to make use of these developments to keep ever more pervasive track of its citizens. Because governments do not normally recognize any legitimate rivals in making legislation for citizens to obey, there is a very real possibility that they will use the information they store for purposes more harmful than helpful to the prosperity of the citizens. With the passage of time and continued improvement in information technology, this possibility metamorphoses into probability and then into certainty.

Private entities are also apt to want to gather and use individuals' personal information, sometimes to the detriment of their clients. Google and Facebook, for instance, certainly have access to a great deal of valuable and private information about their users that they could sell to

third parties whose awareness of said information may be unwanted by the individuals it concerns. However, the danger posed by these activities is fairly small since individuals associate with private entities on a purely voluntary basis. If one does not like how Facebook handles one's data, one need not be among their members. Private entities are subject to competition. What makes government misuse of private data so detrimental is that it is much harder and sometimes impossible to "disconnect" from one's government.

What stands in the way of this desire for ever-increasing surveillance is not so much the courage of whistle-blowers such as Edward Snowden, even though they are assuredly integral to the dissemination of wrongdoings. It is thanks to such dissemination that Americans are even aware that they have been spied upon by their own government, or that the Chinese government had to admit to deaths from mining disasters, for instance, which would otherwise have been kept secret. Rather, an array of institutional features is what may block the proliferation of the surveillance state, to the extent that these institutional features are present. In their absence, the low price of information storage and retrieval will continue to tempt states into misusing data. Although legislation that punishes it is in everyone's general interest, it is in no-one's special interest. But in politics, special interests dominate the general interest.

Hence, the character of the heroism of information leaks like Snowden depends in great part on the consequences of their actions for legislation, which in turn depends on an array of institutional features. This essay argues, firstly, that Snowden and leaks like him are indeed heroes for revealing government wrongdoings, and secondly, analyses the character of this heroism by going into some detail on those institutional features that make legislation sensitive to information leaks, and those features that are likely to withstand them.

The structure of the remainder of this essay reflects these arguments as follows: Section II draws on economics to analyse who will best manage rights to personal information and finds that this is generally the individual to whom the information refers. When this state of affairs is violated, individuals taking steps to rectify it are heroes by anyone's definition. Section III considers the social value of this heroism using more economics, essentially arguing that institutional features that incentivize citizens to behave more like consumers increase the positive consequences of information leaks. Section IV summarizes and concludes.

**II – Hallmarks of a Hero**

Who owns private information is an important part of the economics of property rights. With property in general, the rights to it are usually argued to be best left with whomever has easiest control over the property (e.g., Alchian and Demsetz, 1973). If A can use B's property without

bounds, he will not take care of it to B's satisfaction. This is why problems of "commons" occur; as individual users are only owners to a very small extent, but users to the full extent, they will overuse resources.

An advantageous feature of the free market is that private property will tend to encourage socially beneficial uses of property as rights are transferred for money in whatever direction enables them to make more money (above, A might sell the property to B, for instance). Since one makes money by providing customers with what they want, this system has clear benefits to society and is the reason F. A. Hayek (1991), drawing on Henry Sumner Maine, preferred the term 'several property' to 'private property', the latter term suggesting a benefit only to the owner, whereas the former term implies widespread benefits.

Adapted to personal information, the economics of property rights holds that individual to whom a piece of information refers will generally have the greatest interest in seeing that the information is used wisely. This may include the voluntary sharing of it with others, typically with trusted parties under competitive pressure to manage the information well. Recurrent incidents of losses of personal information managed by non-competitive non-proprietors, such as the neglectful handling by the British government of 25 million child benefit records on compact discs in 2007[1], are a case in point. Exceptions to this rule may occur when the information can prevent harm done to others, but even here control may be best left with the individual; though it clearly harms others not to know if a person is HIV positive, for instance, legislation that mandates the sharing of such information can backfire if it prevents people from getting tested.

In the case of Snowden's revelations, it turned out that the American National Security Agency (henceforth called the NSA) had collected metadata on communications between Americans. This means that the *content* of communications was not gathered, but their frequencies and lengths and of course the people involved were. Such information is sufficient to establish many intensely personal things about people, such as who contacts religious, medical, or adult establishments (wherever a contacted establishment serves a narrow purpose, inference about the contacting individual is rather an easy matter), as has been established in fieldwork by Meyer and Mutchler (2014), who ask voluntary participants to provide data on their telephone contacts through a smartphone application.

In this way, one can liken government surveillance to a sort of in-kind taxation, akin to the draft or to the taking of private land for public use, the practice known as eminent domain, compulsory purchase, or expropriation, in some of their various incarnations around the world. In-kind taxes are

[1] For a Q&A on the incident by the British Broadcasting Corporation, see: 'Q&A: Child Benefit Records Lost', Last updated on 22nd November 2007: http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm (accessed on 10th November, 2015).

notoriously pernicious because – unlike taxes paid in money – there is no way for the taxed individual to choose where the burden falls: “Economic values are less important to us than many other things precisely because in economic matters we are free to decide what to us is more, and what less, important” (Hayek, 1944, p. 68).

The burden of the tax that government surveillance of citizens represents may fall in highly complex and unexpected ways. For one thing, if one’s file happens to contain, say, phone calls to adult establishments and this file is lost by the government, one could find oneself subjected to blackmail for the rest of one’s life if the file falls into the wrong person’s hands. Moreover, how much one “pays” is apt to depend to a great extent on who one is and one’s relation to persons of influence. If surveillance leads to the incarceration or the killing of “suspects”, counter-reactions against the government are less likely if the “suspects” were not of the same nationality as the incarcerating or killing government, or were part of a disliked minority. Such individuals pay more.

Many individuals who, for research purposes, out of curiosity, or in some other harmless way, have visited the websites of, or made phone calls to, organizations looked upon with suspicion by the government will sleep uneasily from the knowledge that their communications are monitored, for in uncertain cases invigilators are likely to tend to choose too much rather than too little investigation and, where deemed necessary, too much rather than too little action; invigilators will be loath to have had the opportunity to prevent some great crime and not taken it. These effects are present even in democracies. Under totalitarian systems, they are of course likely to be more of a norm than “isolated incidents”.

Lastly, the spying that governments orchestrate may be carried out *in secret*. This was certainly the case in Snowden’s revelations of the NSA’s activities, the extent of which are still not fully known, and heightens the aforementioned uncertainty since unsuspecting individuals would not have taken any care at all when communicating before the revelations. These revelations are therefore likely to trigger avoidance behaviours among individuals particularly averse to the idea of being spied upon and among individuals who believe they may be targets for spy operations. This can happen even in the absence of such programmes because individuals will believe the presence of further, undiscovered, secret operations more likely when similar operations have been revealed. The point is that avoidance (through encryption or in other ways) is costly and their scope will be greater when the extent of surveillance operations is not known.

The usual rejoinder offered against concerns of privacy and property given above is that they are required on consequentialist grounds in order to avoid the horrible dangers of the day (often violent ideologies such as Islamism, Naziism or Communism), usually labelled as threats to national security. While many citizens will be upset at the many harmful effects of being spied on, they might consider

surveillance acceptable if it prevents, say, acts of terrorism, crime, or military secrets being leaked to foreign powers. The problem with this rejoinder is that it considers neither the efficiency of, nor the alternatives to, the means whereby one wishes to avoid them.

Firstly, the gains from protection against these types of dangers, even by the highly invasive means of the NSA or organizations using similar methods, are frequently overstated, so much so that, cheap though surveillance has become, any resources spent on avoiding them are likely wasted even if one disregards the costs of lost privacy. Reports to the effect that deaths from traffic accidents vastly outnumber deaths by terrorism are legion (see, e.g., Wilson and Thomson, 2005), and frequently estimate risks of the former to be hundreds of times greater than those of the latter. Surveillance is surely more worthwhile in the case of crime, but *mass* surveillance treats everyone as a suspect when court orders to monitor and search select individuals on reasonable causes are readily available and yield more plentiful information than the NSA's metadata.

Secondly, neutrality on the international scene may prove more successful than widespread surveillance at reducing threats to national security. Casual evidence for this proposition is that traditionally neutral countries like Switzerland appear to face no significant threat to national security. Of course, increased neutrality also means that one cannot advance national causes globally, but it is questionable whether such actions have ever tended to bring about positive and lasting results; Easterly *et al.* (2008) find that military interventions, even when carried out by the US and during as well as after the Cold War, have tended to *reduce* democratic status in the countries subjected to the intervention; Dean and Leeson (2009) find evidence that neighbours "catch" only about eleven per cent of other countries changes in democratic directions, indicating that "nation building" is a poor way of advancing democracy even when democracy is successfully established; and Boettke and Coyne (2009) argue that there are no good theoretical reasons to expect foreign intervention to succeed in the absence of a way for the intervening power to credibly commit to long-term support of reformed institutions (which can be very costly, indeed, as illustrated by the cases of Iraq and Afghanistan).

Thus, the arguments for widespread surveillance programmes appear to rest on unsound foundations. The advantages of letting the property rights to personal information remain with the individuals to whom the information refers are far more tangible than the suggested perils of not doing so. Whenever an individual is in a position to reveal wrongdoings by the government in this area and chooses to do so, he can only reduce the likelihood that people will suffer from the ills, firstly, by simply raising awareness that wrongdoings occur and affect many people, and secondly, by possibly impacting public opinion to demand that the wrongdoings stop. This completes the economic case against mass surveillance.

Having an economic case against mass surveillance makes it easier to see that there is also a strong moral argument against it. The moral argument could differ from the economic one only if there were reasons to believe it right to violate property rights even when doing so is to the detriment of society. This is tantamount to advocating the violation of property rights for its own sake, "though the heavens fall". Some theories of normative ethics, notably the utilitarian-consequentialist ones, think it right to violate property rights when doing so yields social *gains*, but certainly not otherwise. Since violating property rights to private information yields social *losses*, doing so is indeed immoral.

With these points in mind, it is clear that exposers of secret government surveillance programmes are exposers of immoral and socially harmful activities. The usual label used for such individuals is that of hero and there is no reason not to apply it to men like Edward Snowden. What remains to be established is the character of his heroism and the heroism of people like him. That is, what changes to legislation and to people's well-being can be expected from this sort of heroism? How "big" a hero is a man like Snowden? This issue is discussed in Section III.

**III – The Extent of the Heroism of Information Leaks**

Revealing wrongdoings is the right thing to do, but the fact is that the harm that was done before they were revealed was likely to the profit of those who did it. This is especially the case the more systematic and established the wrongdoing is, and suggests that acts of whistleblowing may "merely" make things known without changing their character. In analogy with professional sports afflicted with the widespread use of performance-enhancing drugs, it could be that democracies continue to use mass surveillance even after their scope has been revealed to the citizenry. This is because mass surveillance (1) benefits the leaders, (2) is cheap given the secular decline in the price of handling big data, and (3) legislation against it is in everybody's *general* interest, but in no-one's *special* interest.

Mass surveillance can persist in spite of revelations of it and in spite of widespread indignation if these three conditions are satisfied. Taking the conditions in turn, mass surveillance most obviously enables ruling politicians to keep track of political opponents and gain information on other individuals to ascertain their usefulness or danger to the present power arrangement. This can only benefit the rulers. The drawback is the risk of exposure, but this is handled by the third condition.

Anyone who has seen a computer from the 1990's knows that today's information technology is vastly superior to the state of the art of two decades ago. Ever-faster processing times means that highly complex information can be retrieved within the blink of an eye. Computers capable of performing these feats sell for less than machines that could only carry out a small percentage of them in the 1990's. This point ties in with the first condition, since increased availability at lower prices should raise the leaders' benefits. But continued improvements in information technology will

make more widespread surveillance still more tempting. Certainly information technology is also used to disseminate its misuse, but here again the third condition stands in the way of hope.

The third condition involves some essential political economy. Firstly, one must dispense with the idea that the government are the servant of the people and will always strive to the increase of their welfare. This is because the individual citizen is merely one voice among many thousands and often millions of others. Therefore, whatever effort he exerts to control public servants has a cost that only he bears, and a benefit shared by everyone. However, there is a benefit only if he can convince a sufficient number of his fellow citizens that they should trust and act on his findings. From the individual's perspective, the costs are clearly going to outweigh the benefits. The result is that the provision of control that politicians carry out the general interest is undersupplied. This has been well-known in the field of public choice since its inception (Black, 1958; Buchanan and Tullock, 1962), and explains why small special interests such as farmers or doctors can impose uneconomical policies on the rest of society.

Some further explication on the point that citizens are unlikely to oust politicians over spy scandals may be useful. However outraged individuals are over revelations of wrongdoings by their own government, the only thing they can do to improve things is to vote for someone else to replace a crooked incumbent. Given the secrecy that typically surrounds surveillance agencies, the incumbent will often be able to claim with some plausibility that he was unaware of the misdeeds and will take steps to limit them in future. But amended legislation is rather an empty gesture considering the fact that what the NSA did already was in clear violation of the US Constitution's Fourth Amendment that prohibits searches and seizures sans probable cause. Moreover, responsibility for any particular wrongdoing in a democracy is typically divided among so many individuals that everyone involved can claim to have been of so little significance to the wrongdoing that it would have occurred anyway and that their support could therefore have been of a justifiably unreflective kind.

A further reason to suspect little reaction by voters to revelations of scandalous surveillance programmes is that personal information in the hands of a small government is nowhere near as bad as personal information in the hands of a large one. Hayek approvingly quotes Leon Trotsky's well-known insight that "where the sole employer is the State, opposition means death by slow starvation. The old principle: who does not work shall not eat, has been replaced by a new one: who does not obey shall not eat" (Hayek, 1944, p. 89). In a nation where the state controls the economy, one had better not displease the political establishment lest one be left without a job, for in such a state the political establishment is one's ultimate employer. Wherever the state does not control the entire economy, it is still a good idea to watch what one says, but not as crucial. The more important an actor is the state, the more damage it can do.

If one were to estimate how much damage state surveillance can do for various degrees of state control of the economy, the damage would be positive but at a minimum for a minimal state. If the state controls the police, one could still be thrown in prison, maybe not for thought-crimes but for some convenient excuse, so that one's employment prospects are still reduced. But the possibilities of fighting this unhappy outcome are far greater when lawyers and civil-rights groups are free of state control and therefore not afraid of helping to avoid such an outcome. In the end it is unlikely that a thought-crime should ruin one's life in a minimal state.

At the opposite end, the small set of adversities that could conceivably happen in a free economy remain possible under maximal state control. But added to this set is a vast array of horrors, because there is no way a lawyer would risk his licence to defend a client against the state and the same goes for civil-rights groups whose members must also depend on the state for sustenance when the state is all-encompassing. If one gets into trouble with the state, there is no alternative employer. Under this sort of régime, a thought-crime is very likely indeed to be ruinous.

Happily, outcomes when the state controls roughly half of the economy (which it can do in very many different ways when there are numerous different sectors and even more possibilities for different regulations and differential taxation) will tend to be much closer to the free-market outcome than to the totalitarian outcome, though many comparatively small legislative quirks can significantly pull the outcome in either direction.

This outcome is due, simply, to the presence of alternatives to state employment. Again, the alternatives are relevant not just for the individual thought-criminal but for those who could defend him. A state controlling half the economy can close roughly half of the alternatives, but different alternatives will appeal to different individuals, so many potential defenders of persons accused of thought-crimes will not see the closed alternatives as losses anyway. However, this also means that a growing government eats away at liberty more quickly when the growth occurs from a higher level. Most Western nations would fall into this category.

What has been said so far indicates that losses of privacy in Western countries may be quite rationally regarded as being of little significance to many individuals. Several studies in fact show that people are not willing to pay very much to have their private information protected. Since these studies are typically carried out in countries with a long tradition of liberal democracy and shares of the economy controlled by the state at about half or less, they do not point to any categorical indifference to privacy but merely to a circumstantial one. Furthermore, personal information in these studies is generally given to private entities rather than states.

For instance, Beresford *et al.* (2012) ask one groups of subjects to choose between purchasing at most one DVD from either of two sellers, one asking for the purchaser's monthly income and date of

birth, the other for his favourite colour and year of birth. The former offers DVDs at a price one euro lower than the latter. The paper finds that virtually no-one buys from the relatively high-priced seller. Moreover, when a different group of subjects choose between the same sellers, who now offer the same prices but otherwise remain unchanged, half of them still choose the seller that demanded relatively sensitive private information.

Readers of papers like this one sometimes are heard to conclude that privacy is not important, but such a conclusion is unwarranted for the aforementioned reasons that these studies lack validity for cases of large and expanding government. The right conclusion is that many individuals do not put a very high value on some aspects of their personal information (witness as further evidence the rise of Facebook, for instance) in the hands of private, competitive entities. More importantly, even if a low willingness to pay to protect one's privacy extends to giving it to the government, that valuation is not a categorical feature of privacy but a consequence of the fact that government today is much less than all-encompassing.

If Facebook, Google, or other private entities can be punished for misusing personal data because it is easy to find alternatives to their services or simply stop using them, government misuse of personal information can be stopped only by many individuals' collective intent on choosing the right politicians. But this choice requires a great deal of effort and the success does not depend on any one individual's participation, so nations are stuck with snoopy leaders. This collective-action problem is at the heart of the affliction of mass surveillance; the individual gets all the benefits from choosing wisely between private entities, but only an infinitesimal share of the benefits when choosing between politicians.

If changing jurisdictions were as easy as switching between Gmail and (say) Hotmail, there would be no collective-action problem and those upset with revelations of misuse of personal information could instantly choose another provider of legislation. The fact that choosing a different jurisdiction is quite difficult, in combination with the aforementioned collective-action problem, unfortunately means that revelations such as those made by Snowden will only have a very limited impact on reducing the scope of the surveillance state. The improvement is not zero, however, because some individuals will think twice before moving to a surveillance state and the odd citizen of such a state may consider leaving. But significant improvement upon the present state of affairs is unfortunately impossible without significantly improved institutions.

Getting such institutions is itself subject to the problem of collective action. Essentially, nations would have to compete for citizens the way small jurisdictions do in Tiebout competition (Tiebout, 1956). Steps in this direction may come by more riches and knowledge, including language skills, which tends to enhance mobility across nations, or by institutional entrepreneurship as in the

establishment of floating cities with detachable parts on the oceans proposed by the Seasteading Institute (Friedman and Taylor, 2012). Only time will tell for sure what comes of developments such as these, but they can potentially greatly influence the impact of revelations such as those by Snowden.

At present, Snowden's heroism is more than merely quixotic; he has raised awareness so that individuals can better protect their privacy from the harmful consequences of state possession. As governments do not typically control more than half of the economy at present, some individuals might not care to protect their information, but others will. Snowden's heroism, unfortunately, does not extend so far as to significantly influence legislation. That would be possible only under institutions very different from the ones we have today. So although Edward Snowden is not quite Superman, at least no-one will mistake him for the Man from La Mancha.

**IV - Conclusion**

Edward Snowden and others who reveal widespread government misuse of personal information are indeed heroes for doing so. They are heroes for three reasons; (1) the collection of personal information by means of invigilation violates property rights and has no net social benefits; (2) it is better to know that one is being spied on than not to know, as this enables citizens to take precautions according to their preferences to protect their privacy, the loss of which varies in magnitude with the size of government; and (3) exposing wrongdoings improves policy, albeit only to a very small extent given the problem of collective action.

The third point above highlights the importance of institutional features in determining the ramifications of the heroic deeds. In a perfect world in which individuals could move costlessly between jurisdictions, leaders caught instituting programmes to spy on their citizens would be in great trouble and change would have to come quickly lest the state's population shrinks precipitously. In a world in which changing jurisdictions is very expensive, the cheapness of information technology and the benefits to political leaders of using it combine to reduce the social benefits of the remarkable bravery of whistle-blowers like Edward Snowden.

**Bibliography**


Alchian, Armen, and Harold Demsetz, 'The Property Rights Paradigm', *The Journal of Economic History*, Vol. 33, No. 1 (Mar., 1973), pp. 16-27.

Beresford, Alastair R., Dorothea Kübler, and Sören Preibusch, 'Unwillingness to Pay for Privacy: A Field Experiment', *Economics Letters*, Vol. 117, Issue 1 (Oct., 2012), pp. 25-27.

Black, Duncan, *The Theory of Committees and Elections*, Cambridge University Press, 1958.

Boettke, Peter, and Christopher Coyne, 'The Problem of Credible Commitment in Reconstruction', *Journal of Institutional Economics*, Vol. 5, No. 1 (2009), pp. 1-23.

Buchanan, James, and Gordon Tullock, *The Calculus of Consent: Logical Foundation of Constitutional Democracy*, Liberty Fund, Indianapolis, IN (1999) [1962].

Dean, Andrea M., and Peter T. Leeson, 'The Democratic Domino Theory: An Empirical Investigation', *American Journal of Political Science*, Vol. 53, No. 3 (July, 2009), pp. 533-551.

Easterly, William, Shanker Satyanath, and Daniel Berger, 'Superpower Interventions and Their Consequences for Democracy: An Empirical Inquiry', *Brookings Global Economy and Development*, Working Paper No. 17 (Jan., 2008).

Friedman, Patri, and Brad Taylor, 'Seasteading: Competitive Governments on the Ocean', *Kyklos*, Vol. 65, Issue 2 (May, 2012), pp. 218-235.

Hayek, Friedrich August, *The Fatal Conceit: The Errors of Socialism* (W. W. Bartley III, ed.), University of Chicago Press, 1991.

Hayek, Friedrich August, *The Road to Serfdom*, ARK Paperbacks, 1986 [1944].

Mayer, Jonathan, and Patrick Mutchler, 'MetaPhone: The Sensitivity of Telephone Metadata', *Web Policy*, March 12th, 2014: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (accessed on November 8th, 2015).

Tiebout, Charles M., 'A Pure Theory of Local Expenditures', *Journal of Political Economy*, Vol. 64, No. 5 (Oct., 1956), pp. 416-424.

Wilson, N., and G.Thomson, 'Deaths from International Terrorism Compared with Road Crash Deaths in OECD Countries', *Injury Prevention* (Brief Report), Vol. 11 (2005), pp. 332-333.