On the Political Economy of Privacy: Information Sharing between Friends and Foes

Roger Congleton

Working Paper No. 15-21

This paper can be found at the College of Business and Economics Working Paper Series homepage:

http://be.wvu.edu/phd_economics/working-papers.htm
I. Introduction

This paper analyzes the personal demand for privacy and its implications for election-driven public policy. Privacy is multidimensional, which makes the demand for it and its opposite, fame, more complex than it might at first appear. It is also a product of social interactions and technology, and so only partially a matter of personal choice. When a person walks through a village, town, or city, his or her exact location is revealed to everyone that sees that person pass by. At this level of analysis, privacy is the joint product of a decision to work through the village undisguised and of the decisions of others to watch and remember what they observe.

In former times, this loss of privacy would occur without technological support. It was the consequence of the effects of reflected daylight on the human eye, the brain’s ability to detect patterns in the data relayed to it via optical nerves, and to record what was seen for future use. Such “invasions” of privacy were not the result of innovations such as street cameras, but of the evolution of sight organs and nervous systems.¹

¹ Posner (1978/9) suggests that “the concept of privacy, in the sense in which we use it today is a Western cultural artifact. The idea that it might be pleasant to be off the public stage was hardly meaningful in a society in which physical privacy was essentially nonexistent--was not only prohibitively costly, but also extremely dangerous.”
Sight and memory have obvious survival advantages, in part because they reduce the privacy of others, making both friends and foes easier to identify. On the other hand, privacy also has survival advantages, because it makes one less likely to be eaten for lunch or otherwise taken advantage of. Evolution thus also supports privacy generating capacities: camouflage coloring, near silent movement, and strategies for using night and shadow as times to move and/or sleep. As counter strategies, many predators have acute detection systems that include night vision, hearing, smell, and “data” processing skills. Natural methods of increasing privacy are always incomplete, although nonetheless useful.

This is partly because of countervailing detection technologies, but also because there are advantages to being recognized by fellow members of the same species and by complementary species. Color, smell, and song are often used to attract a mate or other symbiotic partner, although such signaling behavior also increases the risk of being noticed by others looking for supper.

For humans, the natural tradeoffs between stealth and signaling remain in evidence today, although less so than in earlier hunter-gatherer times. In human societies, the natural tradeoffs are compounded by losses and benefits associated with a variety of conflicts and complementarities associated with life within various organizations. Secrecy often reduces conflict and increases the likelihood of success. Signaling, however, is often necessary to obtain support from fellow team members, mates, and employers, at the same time that it may increase risks associated with publicity. The optimal level of privacy in nature and in human society is complex and context specific.

This paper uses rational choice models to shed light on some essential properties of the relevant tradeoffs and how they affect both private choices and public policy. The models developed focus on two areas of privacy linked by detection technologies. The next section of the paper models private tradeoffs between stealth and signaling, these are used in the subsequent sections to explore implication for government policies. The results can easily be extended to multidimensional settings.
II. Some Simple Analytics of the Demand for Privacy

As a point of departure, suppose that a person, Al, has two strategies for affecting her privacy: stealth (H) and signaling (S). The first increases privacy by reducing the probability that she is detected by others. The second reduces privacy by increasing the probability that she is discovered by others. Assume also that there are two other types of persons in the community of interest: friends and foes. Meeting friends always produces benefits and meeting foes always produces losses. Average losses imposed by foes are denoted L and average benefits from finding friends are denoted B.

The probability of being detected by one's friends and enemies may be different for various reasons, including different detection strategies and abilities, the relative numbers of friends and foes, and technology. These probabilities are represented as: \( F = f(H, S, N^F, D^F, t) \), where \( N^F \) is the number of friends and \( D^F \) is their average effort at detection, and \( E = e(H, S, N^E, D^E, t) \). In both cases, the probability of detection decreases with stealth (H), increases with signaling (S), the detection efforts of friends and foes (\( D^F \) and \( D^E \)) and their numbers (\( N^F \) and \( N^E \)). Both functions are assumed to be strictly concave. In addition, the technology of detection (t) tends to increase the success rate of detection, although at diminishing rates. Al's privacy can be regarded as her overall probability of being detected, E+F. Complete privacy requires both F and E to be equal to zero, which may not be feasible (in all dimensions), given the costs involved, the efforts of others, and relevant technology.

A privacy-choice environment is characterized by these two probability functions and the gains and losses associated with discovery by friends and foes, the cost of stealth and signaling technology. The expected net benefit of Al's privacy strategies in such a choice environment is:

---

2 The third strategy, detection is neglected in the first part of the paper. It can indirectly increase privacy by reducing the amount of signaling that must be engaged in to find a friend. Insofar as enemies can also be detected, and hiding/stealth adjusted in response, it may also improve somewhat improve the effectiveness of hiding. These effects are neglected in the first sections of the paper in order to focus on the detection efforts of others.
\[ N^* = f(H, S, N^F, D^E, t)B - e(H, S, N^E, D^F, t)L - \epsilon(H, S, t) \]  

Al’s optimal combination of stealth and signaling, \( H^* \) and \( S^* \), are characterized by two first order conditions:

\[ N^*_{H} = -e_{H}L - (-f_{H}B + c_{H}) = 0 \]  
\[ N^*_{S} = f_{S}B - (e_{S}L + c_{S}) = 0 \]

with: \( f_{H} < 0, e_{H} < 0, c_{H} > 0 \)  
\( f_{S} > 0, e_{S} > 0, \text{ and } c_{S} > 0 \)

Expected marginal benefits from each of the strategies should be set equal to the expected marginal costs. Figures 1a and 1b depict typical solutions. Part of the cost of stealth is the reduced probability of being found by a friend. Part of the cost of signaling is the increase probability of being found by a foe. In an environment that includes both friends and foes, Al is not likely to have an interest in complete privacy or extreme fame.

The implicit function theorem allows the optimal combination of stealth and signaling to be represented as functions of parameters of the choice setting:

\[ H^* = h(B, L, D^F, D^E, N^F, N^E, t) \]  

4
H* can be thought of as the private demand for privacy and S* as the demand for its opposite, the demand for fame; although it is the detection probabilities that actually produces privacy and fame.  

Privacy is only partly controlled by the individual, because it also depends on the detection rates of one’s friends and foes, and the available technologies for stealth, signaling, and detection.

The interdependence between stealth and signaling arise through the probability of detection functions. As constructed, however, the probability of detection functions do not include loss or benefits as arguments. This mathematical independence allows partial derivatives of H* and S* with respect to B and L to be calculated separately by applying the implicit function differentiation rule to equations 2.1 and 2.2. The results are consistent with economic intuition:

\[ H^*_L = \frac{-e_H}{-N^e_{HH}} > 0 \]  \[ 4.1 \]

\[ H^*_B = \frac{f_H}{-N^e_{HH}} < 0 \]  \[ 4.2 \]

\[ S^*_L = \frac{-e_S}{-N^e_{HH}} < 0 \]  \[ 4.3 \]

\[ S^*_B = \frac{f_S}{-N^e_{HH}} > 0 \]  \[ 4.4 \]

The privately optimal extent of signaling (S*) increases as expected marginal benefits from friends increases, and falls as marginal expected losses from enemies increases. The privately optimal level of stealth (H*) decreases as expected marginal benefits from friends increase and increases as marginal expected losses from foes increases.

If the probability functions are assumed to be separable, partial derivatives can be calculated in the same manner for the other parameters of Al’s choice environment.

---

3 Fame in this context is the probability of being detected (recognized), which is the sum of F* and E*. See Cowen (2000) for an innovative analysis of the fame industry in contemporary society.
(otherwise matrix techniques have to be applied). Stealth is focused on below, to save space. Those for signaling are very similar, but have opposite signs.

\[ H'_{DF} = \left[ F_{HDF} B \right] / \left[ -N_{iHH}^e \right] < 0 \]  \hspace{1cm} (4.5)

\[ H'_{NF} = \left[ F_{HNF} B \right] / \left[ -N_{iHH}^e \right] < 0 \]  \hspace{1cm} (4.6)

\[ H'_{DE} = \left[ -E_{HDE} L \right] / \left[ -N_{iHH}^e \right] > 0 \]  \hspace{1cm} (4.7)

\[ H'_{NE} = \left[ -E_{HNE} L \right] / \left[ -N_{iHH}^e \right] > 0 \]  \hspace{1cm} (4.8)

\[ H'_{t} = \left[ -E_{HtL} + (F_{HtB}) \right] / \left[ -N_{iHH}^e \right] <> 0 \]  \hspace{1cm} (4.9)

Derivatives with respect to these other parameters of the risk environment are also intuitive. Stealth (hiding) falls as parameters that increase the probability of detection by a friend increase, as with friendly detection efforts and numbers of friends. Contrariwise, stealth decreases as the number of foes and/or their detection efforts increases.

Generalized informational technology, however, has an ambiguous effect on stealth, because it affects both the expected marginal benefits of being discovered by a friend and expected marginal losses from being discovered by a foe. If the probabilistic effects of technology are similar in magnitude, it is the relative size of the marginal benefits from friends and marginal losses from enemies that will determine the change. In cases in which technology improves the detection efforts of enemies more than friends, stealth tends to rise, assuming losses from discovery by enemies are similar in magnitude or larger than the benefits of discovery by friends. The effects of these variables on signaling efforts mirror those on stealth, with signaling increasing in an environment becomes more friendly (as \( N^e \) or \( D^e \) increase) and decreasing as the environment becomes less friendly (as \( N^e \) or \( D^e \) increase). Technology, has ambiguous effects on optimal signaling, for reasons similar to its affect on optimal stealth.

Of course, not all environments have interior solutions in stealth or signaling. Stealth, for example, would not be undertaken in a world in which only good things follow
from being discovered (a world without foes). Signaling would not be undertaken in a world or area of life without friends.⁴

Overall the results affirm the hypotheses developed in the introduction: that the demand for privacy is context specific, rather than absolute, and that persons may simultaneously engage in behavior that increases and diminishes privacy (stealth and signaling).

Equilibrium levels of privacy emerge from the decisions of all persons in a community, and can be approximated as a Nash equilibria. The stealth and signaling strategy functions are best reply functions. As true in other non-cooperative games, the result may be more or less privacy than in the joint interests of all members of the community.

III. Governments and Privacy

We now shift from a private choice setting to a public choice setting and assume that governments know the best reply functions of their citizens.

Governments undertake a broad range of policies that affect privacy, and the extent to which these increase or decrease privacy varies with the type of government. Governments can be a fiend or a foe, depending on the purpose and effects of detection on the persons of interest. For example, a democratic government (without agency problems) might help citizens avoid detection by potential foes in their communities. It can do so by discouraging detection efforts by and reducing the number of foes by imposing penalties on persons that invade a person’s privacy in order to impose losses, as with thieves, child molesters, con artists, computer virus engineers, and identity thieves.

Other policies may support the detection effort of potential friends, as with the creation of market squares, zoning for market districts, the provision of public paths and highways, and so forth. Subsidies for telecommunication services and the internet are recent examples of “connecting” or detection services that tend to increase the probability of detection by friends (albeit also somewhat by foes).⁵

---

⁴ For example, a person who just wants to be left alone for the moment, can be regarded as one that regards all other persons to be foes, for the period of interest.

⁵ The use of eminent domain to create right of ways for utility companies has clearly
Except for the cost of doing so and disagreements about who friends and foes are, the ideal privacy policies would produce a zero probability of detection by those who intend to harm those detected (foes), and a hundred percent probability of being detected by those who intend to confer benefits (friends).

Nonetheless, even if there are policy areas in which privacy policies can produce net benefits for most citizens, there is no guarantee that such policies would be adopted. Governments can be a foe as well as a friend, and there may be privacy tradeoffs among policies. The raising of taxes or criminal investigations, for example, may involve reductions in privacy (audits and data mining) that are greater than many citizens demand. With this in mind, the next sections of the paper examines the privacy policies of extreme types of governments.

A. Optimal Detection for Leviathan

As an extreme case, consider the behavior of leviathan in its efforts to maximize revenue from its citizens. In the present setting, leviathan does not know the wealth or income of its potential tax payers, but uses direct and indirect detection methods to try to discover its tax base. The government knows that citizen taxpayers will attempt to avoid detection by agencies that impose losses, as in equation 3.1 above. Suppose that the society of interest has M members and that leviathan imposes a lump sum wealth tax of average amount L, but which is bounded by the wealth discovered. Expected net revenues given the tax avoiding (hiding) efforts of the citizenry in their dealings with the government can be represented as:

\[ R^e = M e(H^*, S^*, 1, D^e, t) L - c(D^e, t) \]  

\[ (5) \]
where $D^* \text{ is the government’s investment in detection for the purpose of collecting revenues, which includes ordinary audits, census counts, and other indirect efforts to estimate wealth or income via consumption or electricity use. } H^* \text{ is the average voter’s effort at stealth, given detection effort } D^* \text{ and tax } L$.

Net revenues are maximized when the leviathan’s detection and tax rates satisfy:

\[
ML(E_H H^*_{DE} + E_{DE}) - C_D = 0 \quad (6.1)
\]

\[
ML (E_H H^*_{L}) + EM = 0 \quad (6.2)
\]

Detection is undertaken up to the point where the expected marginal increase in revenues (net of increased avoidance) equals the marginal cost of detection efforts. Since tax payers realize only losses from being detected by leviathan, signaling is not invested in, $S^* = 0$ nor affected by leviathan’s detection efforts. The marginal cost of detection includes two components, its direct marginal cost ($C_D$) and the indirect reductions in revenues generated by inducing greater effort to hide taxable income by those the detection is deployed against ($MLE_H H^*_{DE}$). An increase in detection efforts tends to increase tax avoidance and thereby the size of the shadow economy.\(^7\) The tax level is set to equate the direct marginal revenue increase with its indirect reduction generated by increases in taxpayer avoidance efforts.

Taxpayer responses imply that detection rates and taxes are lower than they would have been without avoidance efforts by taxpayers.\(^8\) Figure 2 illustrates leviathan’s optimal detection efforts as a Stackelberg equilibrium, with private responses taken into account.

---

\(^7\) See Schneider and Enste (2000) for an overview of the foundational literature on shadow economies.

\(^8\) Security risks to the regime are neglected here in order to focus on Leviathan’s economic interest in surveillance and auditing programs. Security interests would increase the optimal level of surveillance insofar as it increases the probability that a given regime retains power.
The implicit function theorem allows leviathan’s optimal detection and tax rates to be represented as a functions of national population, the average revenue recovered, and the state of detection technology.

\[ D^* = d(M, L, t) \]  \hspace{1cm} (7.1)

\[ H^* = h(0, L, 0, D^*, 0, 1, t) \]  \hspace{1cm} (7.2)

Leviathan’s response to changes in its decision environment is characterized by the partial derivatives of equation 7.1:

\[ D^*_M = \frac{[E_M^H H_{D}^* + E_D^H]L}{-R^D_D} > 0 \]  \hspace{1cm} \text{if } H^* \text{ effects are relatively small}  \hspace{1cm} (8.1)

\[ D^*_L = \frac{M(E_M^H H_{D}^* + E_D^H) + M L e_H H_{DL}^*}{-R^D_D} > 0 \]  \hspace{1cm} \text{if } H^* \text{ effects are relatively small.}  \hspace{1cm} (8.2)

\[ D^*_t = \frac{M (E_M^H H_{D}^* + E_D^H + E_D^H) - C_D}{-R^D_D} > 0 \]  \hspace{1cm} \text{if } H^* \text{ and cost effects are relatively small}  \hspace{1cm} (8.3)
The partial derivatives Leviathan’s detection efforts cannot be signed without making further assumptions about the extent to which citizens engage in efforts to hide from their government’s detection efforts. In cases in which the various taxpayer responses (the derivatives of H*) are relatively “small,” Leviathan’s behavior is predictable. An increase in the number of potential taxpayers tends to increase detection efforts. Similarly, an increase in average expropriation yields (L) encourages greater detection efforts. An improvement in the technology of detection also tends to increase efforts if its effect on marginal costs is relatively small or negative. In such cases, the effect of increased detection on revenue dominate the marginal cost of detection efforts and efforts to avoid detection.

Privacy in spheres of life in which leviathan has financial interests tend to be relatively low, and privacy increasing efforts by citizens (H) tend to be relatively high in the dimensions of choice that affect Leviathan’s ability to tax them or confiscate their goods and services.

It bears noting that if taxpayer responses are relatively large and effective relative to marginal tax yields, the signs of the above partial derivatives may be reversed. For example, in some countries it may be very easy to shift potentially taxable income or wealth abroad in a manner not easily detected, and/or into the shadow economy. If increased detection can be countered by increased stealth, (net) marginal revenues from increased detection is close to zero (or negative), and relatively low detection effort would be engaged in by leviathan. In such cases, leviathan might rely upon other revenue sources to fund its activities.9

In either case, equilibrium citizen responses to detection rate, D*, is determined as above. Privacy in the fiscal relevant dimension of choice is simply: H* = h(0, L*, 0, D*, 0, 1, t). Private economic activity under Leviathan tend to be relatively secret enterprises, because government in such cases is clearly a foe, not a friend.10

---

9 Congleton and Lee (2009) suggest that rent-extraction can provide an alternative to taxation, when taxes are difficult to collect.

10 The analysis focuses on the behavior of a typical member of the community. It bears noting that dictators, unlike leviathan, require some minimal level of support to retain office. Allies and supporters of the government would regard government to be their friend, and therefore engage in signaling to receive benefits (gifts or rents) associated with their dictator’s favor. This aspect of rule
In general, governments that exhibit significant agency problems will adopt detection strategies that tend to undermine rather than advance the privacy interests of their citizens.

**B. Privacy in Democratic Regimes without Agency Problems**

In democracies, elections tend to align the interest of government with the median member of the electorate. Citizens demand a variety of services from their services, many of which affect their sphere of privacy. Policies that explicitly advance the privacy interests of voters tend to reduce the probability that voters (in the majority) will be detected by foes and increase the probability that they find friends. The former policies tend to increase privacy in relevant dimensions and the latter to reduce it. Many other policies have indirect effects on privacy.

The policy choices analyzed below are fiscal ones analogous to those faced by leviathan above, except that in this case citizen-taxpayers receive services as well as pay taxes to their government. It will be assumed that both taxes and benefits from government programs are largely automatic, as might be said of tax collection under a VAT or income tax system, and distribution of benefits through the production of public goods and broad social insurance programs. In addition to these formulaic taxes and benefits, however, there are others that are conditional on detection.

Tax avoidance strategies (stealth) can be exercised on income, which implies that some taxes are paid only if one is audited or income (or sales) are discovered through other criminal investigations. Similarly, some benefit programs are less automatic than others, and require governments to recognize that persons are eligible for them. In the United States, examples include unemployment insurance, instate tuition for college, and a variety of tax

---

11 Indeed, with appropriate constitutional constraints on the majority, all citizens may expect to receive net benefits from such governments (Buchanan and Tullock 1962).

12 Most democratic governments are constitutionally prohibited from simply taking anything that they want by various “takings” clauses, which may explain why they rarely use lump sum taxes.
credits and preferences. A democratic government’s detection and recognition policies thus have significant effects on expected taxes and benefits.

Two detection regimes are analyzed below: first, one in which the information used for tax collection is separate from that used to identify and distribute conditional benefits, and second, a regime in which the same data are used for both conditional taxes and benefits.

**Stove Pipes: Separate Detection Methods and Data**

The median voter model is used to characterize the policies that emerge in a democracy in the absence of agency problems. In this case, the median voter’s tax burden (τ) can be thought of as her share (σv) of the cost of general and conditional government programs. G the total expenditure on the uniformly provided service. F* is the probability that a beneficiary is discovered and awarded a grant, so the cost of targeted benefit programs that confers average benefit, B, in a community of size, M, is F*MB. Similarly, E* is the probability that one’s tax evasion is detected, so in a community of size M in which the fines and supplemental taxes average, L, the expected conditional revenues are E*ML. Thus the median voter’s tax burden is τ = σv [γ(F*MB + G, Df, Df, t) - E*ML], where γ is the cost function for services and detection, which includes administrative and distributional costs.

General government services are assumed to generate benefits that vary somewhat among individuals and are subject to diminishing marginal returns [Uv(G)].

The first case analyzed is that in which government uses separate detection regimes for its tax collection and benefit conferring programs. The magnitude of detection efforts for the conditional benefit and tax-collection programs are Df and De. Given the government’s policies and efforts at detection, voter-taxpayers will engage in their privately optimal levels of tax avoidance (H*) and signaling to obtain conditional benefits (S*). In this case, the median voter’s expected net benefit from governmental detection, taxes, and services can be characterized as:

\[
N^* = f(H^*, S^*, Df, t)B - e(H^*, S^*, Df, t)L - c(H^*, S^*) + u(G)
\]
and her ideal vector of government services, conditional benefit and tax programs, and
detection services satisfy:

\[ N^G_G = U_G - \sigma^\gamma [\gamma_G] = 0 \quad (10.1) \]

\[ N^G_DF = F_{DE}B + (BF_H - C_H)H^*_{DF} + (BF_S - C_S)S^*_{DF} 
- \sigma^\gamma [MB\gamma_G F_H + \gamma_{DF} - MLE_H] (F^*_{DF} + S^*_{DF}) = 0 \quad (10.2) \]

\[ N^G_DE = -E_{DE}L + (LE_H - C_H)H^*_{DE} + (LE_S - C_S)S^*_{DE} 
- \sigma^\gamma [MB\gamma_G F^*_{DE} + \gamma_{DE} - E^*_{DE} ML](F^*_{DE} + S^*_{DE}) = 0 \quad (10.3) \]

\[ N^G_B = F - \sigma^\gamma [\gamma_0(FM)] + (FH H^*_B + F_S S^*_B)B 
- (EH H^*_B + ES S^*_B)L \]

\[ \sigma^\gamma [\gamma_0(FH H^*_B + F_S S^*_B)MB] - (CH H^*_B + C_S S^*_B) = 0 \quad (10.4) \]

\[ N^G_L = -E - \sigma^\gamma [EM] + (FH H^*_L + F_S S^*_L)B 
- (EH H^*_L + ES S^*_L)L 
- \sigma^\gamma [(EH H^*_L + ES S^*_L)ML] - (CH H^*_L + C_S S^*_L) = 0 \quad (10.5) \]

These first order conditions can be thought of as a series of expected marginal benefit and
marginal cost calculations. The entire system of equations will hold simultaneously at the
median voter’s ideal point.\(^\text{13}\) The high degree of separability implicit to the net-benefit
approach allows many of the first order conditions to be analyzed one at a time.

Ideal levels of ordinary government services are characterized by equation 10.1,
which is the simplest of the first order conditions. It states that the median voter’s ideal
public service level sets her marginal benefits \((U_G)\) equal to her share of the marginal costs
for providing it \((\sigma^\gamma [\gamma_G])\). Interdependencies with the other decisions exist if detection
efforts affect the marginal cost of those government services.

\(^\text{13}\) The existence of a multidimensional median voter requires a high degree of symmetry in the
distribution of voter ideal points (Plott 1967) or institutions that generate such equilibria one
dimension at a time.
The first order conditions for the size of the conditional programs and their associated detection efforts are far more complex, because each of these induce a variety of stealth and signaling responses on the part of the citizenry. The results of the model of stealth and signaling developed above suggests that targeted benefit programs and efforts to find persons eligible for such programs will induce an increase in signaling behavior and a decrease in stealth efforts. Persons will voluntarily fill out forms that include all manner of private information, wait in long lines, agreed to be interviewed in order to increase their prospects for obtaining the conditional benefits or grants.

Changes in conditional taxes have similar but opposite effects on signaling and stealth efforts. Conditional taxes tend to decrease signaling and increase stealth. Stealth (H) may take the form of poor or secret records, increased use of cash for ordinary transactions, and increased use of services available from the underground economy. As a consequence, conditional benefit programs tend to reduce the demand for privacy, whereas conditional taxes tend to increase it.

A rational voter’s ideal combination of detection and conditional tax and grant programs, in principle, takes all such adjustments into account. Thus the size of the underground economy and privacy for moderate voters are both endogenous to political decisionmaking process; although as modeled, private adjustments are made after the policies are adopted.

Big Data: Integrated Detection Methods

In the above setting, detection and information gathered are assumed to separate programs, with an effective “firewall” between them. The information collected was used for a single purpose, tax collection or benefit dispersal. Such data partitions are less common today, because of recent innovation in software for combining records and reductions in the cost of data storage, integration, and mining, what is being called “big data.” With the advent of the “big data” technologies, all detection efforts become part of one unified recognition and information processing system.

Because of this, the technological shift to “big data” is likely to unsettle previous political (and private) equilibria with respect to privacy. The previous model can be adjusted
to account for “big data” by replacing $D^E$ and $D^F$ with a single detection level, $D$. The median voter’s expected net benefit equation becomes:

$$N^* = f(H^*, S^*, D, B) - e(H^*, S^*, D, L) - c(H^*, S^*) + u(G) - \sigma \gamma(FMB + G, D, D, \theta) - EML$$

(11)

and her ideal level of government detection activities now satisfies:

$$N^*_D = FDEB - \sigma \gamma_D + (BFH - CH)H^*_DF + (BF_S - CS)S^*_DF - EDEL - \sigma \gamma_D - EML + (LEH - CH)H^*_DE + (LE_S - CS)S^*_DE = 0$$

(12)

Note that equation 12 combines the effects of equations 10.2 and 10.3 above. The other first order conditions remain (notationally) as above, although they have slightly different interpretations.

Insofar as the equilibrium in the previous choice implied higher detection rates for distributing benefits than for collecting taxes, $D^F > D^E$, the new optimal detection rate will tend to be between those levels, and far less than the sum of those previous efforts $(D^* < D^F + D^E)$. The result of “big data,” ceteras paribus, tends to be a net increase in privacy in the area in which audits occur and a decrease the areas in which conditional benefits are handed out, as illustrated in figure 3. The marginal losses from audit programs are now partly offset by gains from conditional benefit programs, but the marginal gains from being determined eligible for conditional benefit programs are now partly offset by marginal losses from conditional taxes. The new audit rate is a convex combination of the former ones.
IV. Constitutional Political Economy: Should Privacy Be Protected?

With respect to the minority interests, contractarians argue that constitutions should advance the interests of all parties covered by them so that essentially all affected persons would agree to their provisions. Here one could well imagine that many persons would prefer not to be subject to the codified privacy norms of the majority, as for example with non-mainstream religious, reading, and leisure practices. The purpose of privacy provisions in a constitution is to broaden consensus and thereby increase legitimacy (Vanberg and Buchanan 1989), as well as to mitigate risks associated with political agency problems.

The above analysis suggests that privacy is partly a consequence of public policy choices of the sort focused on by the public finance and law and economics literatures, and partly of individual decisions with respect to signaling, stealth and detection given those policies.

In principle, a government’s detection programs can advance a broad range of voter interests, although as the leviathan case illustrates, it needn’t do so. In the case in which severe political agency problems exist, limiting detection regimes reduces leviathan’s ability
to collect taxes (confiscate wealth) though fine-grained targeted tax systems. That tax-related detection levels tend to be greater under leviathan than under democratic rule is indicated by equations 6 and 10.3. Under leviathan, detection levels satisfies:

\[ M (E_H H^*_{DE} + E_{DE})L - C_D = 0 \]  

while the median voter’s they satisfies:

\[ -E_{DE}L + (L_E H - C_H)H_{DE} + (L_E S - C_S)S_{DE} - \sigma^* [MB\gamma_6 F^*_DE + \gamma_{DE} - E^*_{DE} ML](F^*_{DE} + S^*_{DE}) = 0 \]  

The principle differences between these two expressions are that the median voter takes account of direct effects of the privacy policies on herself. The first order conditions for tax-related detection are otherwise very similar. The last term in equation 13.2, the effect of detection on tax revenues, is the same as that for leviathan, except for the signaling effects. The other terms represent marginal cost effects that the median voter bears, but leviathan does not. The first involves increased chances of paying additional taxes, the second the reduction in the probability of receiving conditional benefits.\(^{14}\)

These additional marginal cost terms imply that the median voter will generally prefer lower detection and revenue levels than leviathan. Bounding detection efforts for tax investigations is thus a method of reducing excessive taxation by increasing privacy. Such limits could well be included as a component of a political or fiscal constitution for this reason alone, given potential losses from political agency problems.\(^{15}\) Other areas of policy in which leviathan would tend to be more intrusive than a well-functioning democracy include those associated with regime security.

Constitutionalizing privacy policies in such instances would be consistent with general interests whenever it is acknowledged that constitutional designs are not likely to perfectly align the interests of government representatives and officials with those of their

\(^{14}\) The survey evidence explored in Feld and Larsen (2012), for example, suggests that tax avoidance would be a reason for voters to prefer less than complete review of tax returns.

\(^{15}\) This difference also partially accounts for the relative size of the shadow economy in authoritarian and democratic regimes that is often discovered (Schneider and Enste 2000).
taxpayer-voters. The analysis above suggests that such constitutional provisions may have to be revisited as innovations in relevant technologies occur.\footnote{\cite{Posner1978/9} discusses a variety of cases in which privacy rights of this sort tend to be protected in civil law.}

V. Conclusions

As true of nature’s costs and benefits, the costs and benefits of privacy in human societies are largely determined by specific circumstances, because the net benefits of remaining undetected varies with the setting, type of activity, and technology. Keeping one’s identity or location secret is clearly more difficult in a village where everyone is known to everyone else, than in a large city where few people know more than a small fraction of the persons around them (or wish to) and even fewer have an interest in “your” present whereabouts and activities.

Technological change can affect the relative costs and benefits of maintaining privacy in different settings. For example, urban areas that install security cameras and face recognition technologies can reduce privacy for individual making use of public spaces as efficiently as village gossips. Counter measures may be induced by such strategies. In a village, one may wear masking clothing or strategically apply make up and hair coloring. In a technological era, one may use various privacy enhancing forms of software on one’s computers and phones, pay for most things with cash, and maintain multiple financial accounts, passwords, and identities.

This paper suggests that the shift to “big data” with its associated storage and data mining technologies has changed both the public and private equilibria in a manner that favors a reduction in aggregate information gathering efforts and an increase in stealth. Restrictions on “big data” may simultaneously reduce the cost of obtaining desired privacy and reduce expected losses from agency costs. However, the model also suggests that concerns about privacy vary according whether one expects to qualify for conditional benefits or be subject to conditional taxes. The issues may be general, but concerns may vary substantially within the population as a whole.
References


