On the Political Economy of Privacy in Communities that Include Both Friends and Foes

Roger D. Congleton
Dept. of Economics
West Virginia University

roger.congleton@mail.wvu.edu

8-4-16

Abstract. This paper develops a conceptual framework for analyzing privacy issues. Neither privacy nor fame are ordinary economic goods. The demand for both are derived from their associated consequences. In some settings privacy is useful, in others not. When applied to privacy relevant public policies, the analysis indicates that there are significant differences between the privacy-relevant policies of authoritarian and democratic regimes. The analysis also demonstrates why technology affects public support for privacy relevant policies. A shift from "stove pipe" to "big data" tends to reduce electoral support for government expenditures on detection activities.

Key Words: privacy, stealth, fame, signaling, big data, political economy of privacy

I. Introduction

Privacy is multidimensional, which makes the demand for it and its opposite, fame, more complex than it might at first appear. People can demand fame and privacy at the same time, although normally for different reasons and often about different matters. Moreover, both privacy and fame are 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 him or her pass by. Privacy and fame are joint products of that person's decision to walk through the village undisguised and of the decisions of others to

watch and remember what they observe. Such natural losses of privacy occur without technological support.[1]

Such "invasions" of privacy are not the result of innovation or public policy, but of the evolution of sight organs and nervous systems. 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. 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 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. Even a stealthy walk through a village may be observed by others even in dim light. Even a stealthy makes a bit of noise and may leave a detectable odor. Such losses of privacy occur partly because of the survival advantages of countervailing detection technologies. Others are products of intent and also reinforced by evolutionary pressures. There are advantages to being recognized by fellow members of the same species and by complementary species. Color, scent, and song are often used to attract a mate or other symbiotic partner, although signaling behavior also increases the risk of being noticed by others looking for supper. A village walk may be contrived to be seen and recognized by undertaking behaviors that draw attention to oneself.

In human societies, biological tradeoffs are compounded by risks associated with a variety of conflicts and complementarities associated with life in organizations and communities. Secrecy often reduces conflict and increases the likelihood of success by

[1] Posner (1978/9) suggests that privacy is a relatively new concept. "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." This seems unlikely to this author. Even in cases in which privacy was prohibitively expensive, it does not imply that it was not demanded. Also, whether it was always prohibitively expensive seems doubtful. Secrets could always be kept and rendezvous in out of the way places were always possible.

generating useful informational asymmetries, surprise.[2] Nonetheless, there are also circumstances in which a bit of fame is helpful. Attracting attention to oneself makes mutually beneficial relationships more likely to develop, at the same time that it increases risks from rivals and predators. Many sellers of goods and services position themselves at prominent places within their communities to attract attention to the goods they offer for sale.[3]

All this points to the fact that both privacy and fame may be demanded by the same person at the same time. This paper develops a tractable mathematical model of such behavior and uses it to examine public policies in democracies and autocracies. Section II models the private tradeoffs between stealth and signaling. Many of the tradeoffs involved can be clarified with a rational choice model of stealth and signaling strategies. Section III uses the model to analyze government policies that attempt to reduce the effectiveness of stealthy strategies or increase the effects of signaling strategies. Perhaps surprisingly, voter-citizens want both privacy increasing and decreasing services from their governments, although the mix that they demand varies with technology and political institutions.

II. A Lean Model of the Personal Demand for Privacy

As a point of departure, suppose that a person has two control variables that affect his or her privacy: hiding (H) and signaling (S). The first increases privacy by reducing the probability that a person's activities or state is detected by others. The second reduces privacy by increasing the probability that the activity or state of interest is discovered by others.[4] In addition, assume that there are two other types of persons in the community of interest: friends and foes. Meeting friends always produces benefits. Meeting enemies (foes)

---

[2] Kuran (1995) suggests that much of human behavior in public is "stealthy" in that it reveals preferences that are not one's true preferences. Stealth includes misdirection as well as efforts to literally hide oneself.

[3] See Cowen (2000) for a thorough analysis of fame and the fame industry in contemporary society.

[4] 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.

always produces losses. Typical benefits from finding friends are denoted B, with $B \geq 0$. Typical losses imposed by foes are denoted L, with $L \geq 0$.

The probability that one's activity of interest is detected by one's friends and one's enemies will often differ. They may use different detection strategies, have different abilities at detection, or exist in different numbers. The probability of being noticed by a friend can be 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. Similarly, the probability of being noticed by an enemy can be represented as $E = e(H, S, N^E, D^E, t)$. In both cases, the probability of detection decreases with one's investment in hiding (H), increases with one's efforts at signaling (S), and with the detection efforts of friends and enemies (D^F and D^E) and their numbers (N^F and N^E). The technology of detection (t) affects both probabilities of being detected, with an increase in technology increasing the rate of detection.

A person's privacy is his or her overall probability of being detected, E+F. Complete privacy thus requires both F and E to be equal to zero. This, of course, may not be feasible (in all dimensions), given the costs of stealth, the efforts of others, and detection technologies. Try as one might, one cannot become completely invisible and silent. Note that the same sum can also be used as an index of fame, with higher totals indicating higher overall fame.

A privacy-choice environment is characterized by these two probability functions, the average gain and loss associated with discovery by friends and enemies, and the cost of hiding and signaling technology. Both conditional probability functions are assumed to be strictly concave to facilitate analysis. The expected net benefit of Al's privacy relevant strategies in a privacy choice environment is:

$$N^e = f(H, S, N^F, D^F, t)B - e(H, S, N^E, D^E, t)L - c(H, S, t) \qquad (1)$$

Given strict concavity, a person's optimal combination of hiding and signaling, H* and S*, can be characterized with two first order conditions:

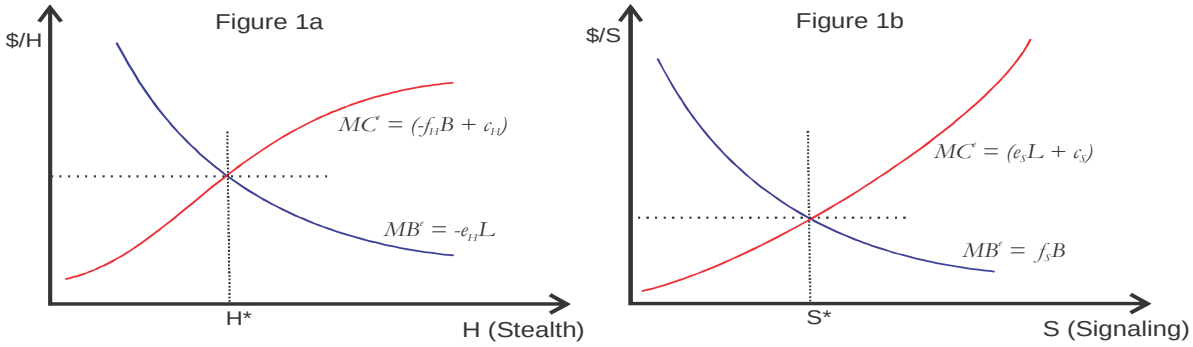
$$N^e_H = -e_H L - (-f_H B + c_H) = 0 \qquad (2.1)$$

$$N^e_S = f_S B - (e_S L + c_S) = 0 \qquad (2.2)$$

$$\text{with: } f_H < 0,\ e_H < 0,\ c_H > 0$$
$$f_S > 0,\ e_S > 0,\ \text{and } c_S > 0$$

As is the case for most activities that can be continuously varied, the ideal hiding and signaling combination sets the expected marginal benefits from each of the strategies equal to their expected marginal costs.

Figures 1a and 1b depict typical solutions. Part of the marginal cost of stealth is the reduced probability of being found by a friend. Part of the marginal cost of signaling is the increase probability of being found by an enemy. In an environment that includes both friends and foes, Al is not likely to have an interest in maximal privacy or fame.



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

$$H^* = h(B, L, D^F, D^E, N^F, N^E, t) \qquad (3.1)$$

$$S^* = s(B, L, D^F, D^E, N^F, N^E, t) \qquad (3.2)$$

H* can be thought of as the private demand for privacy and S* as the demand for its opposite, the demand for fame.[5]

[5] Fame and privacy in this context correspond to the probability of being noticed. Signalling makes that more likely, stealth makes it less likely. This papers address only what might be regarded as local privacy or fame, although the functional forms of the probability of detection functions are general enough to include industrial factors. For example, F_S can be considered the marginal increase in personal fame generated by signaling efforts, broadly construed.

However, privacy is only partly controlled by the individual. It is generated jointly by a person's own behavior, the detection efforts of one's friends and enemies, and the available technologies for stealth, signaling, and detection.

As constructed, the probability of detection functions do not include losses or benefits as arguments. This assumed 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 largely consistent with economic intuition:

$$H^*_L = [\ -e_H\ ) / [-N^e_{HH}] \quad > 0 \qquad (4.1)$$

$$H^*_B = [\ f_H\ ) / [-N^e_{HH}] \quad < 0 \qquad (4.2)$$

$$S^*_L = [\ -e_S\ ) / [-N^e_{HH}] \quad < 0 \qquad (4.3)$$

$$S^*_B = [\ f_S\ ) / [-N^e_{HH}] \quad > 0 \qquad (4.4)$$

The privately optimal extent of signaling (S^*) increases as typical benefits (B) from friends increases, and falls as marginal expected losses (L) from foes increases. The privately optimal level of hiding (H^*) decreases as expected marginal benefits (B) from friends increase and increases as typical losses (L) from foes increases.

If the probability functions are assumed to be separable, partial derivatives can be calculated for the other parameters of a typical choice environment using the single-equation version of the implicit function differentiation rule (otherwise matrix techniques have to be applied). Hiding is focused on below, to save space. Those for signaling are very similar, but have opposite signs.

$$H^*_{DF} = [\ F_{HDF}\ B\ ] / [-N^e_{HH}] < 0 \qquad (4.5)$$

$$H^*_{NF} = [F_{HNF}\ B\ ]/ [-N^e_{HH}] < 0 \qquad (4.6)$$

$$H^*_{DE} = [-E_{HDE}\ L] / [-N^e_{HH}] > 0 \qquad (4.7)$$

$$H^*_{NE} = [-E_{HNE} L] / [-N^e_{HH}] > 0 \qquad (4.8)$$

$$H^*_t = [-E_{Ht}L + (F_{Ht}B)] / [-N^e_{HH}] <> 0 \qquad (4.9)$$

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

An improvement in generalized informational technology 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 through effects on the two probability of being detected functions. If the marginal 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 net effects and an individual's response. In cases in which technology improves the detection efforts of enemies more than friends, stealth (hiding) 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^F or D^F 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 effect on optimal stealth.

Of course, not all environments have interior solutions in stealth or signaling. Hiding, for example, would not be undertaken in a setting in which only good things follow from being discovered (a world without effective enemies). Signaling would not be undertaken in a world or area of life without friends.[6]

Overall the results are consistent with the hypotheses developed in the introduction and with economic intuition. The demand for privacy is context specific, rather than

[6] 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.

absolute, and persons may simultaneously engage in behavior that increases and diminishes privacy (stealth and signaling).

The stealth and signaling demand functions can be regarded as best reply functions in a privacy-detection contest. Equilibrium levels of privacy emerge from the decisions of all persons in a community and can be represented as a Nash equilibria. 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.[7]

III. The Political Economy of Privacy

We now shift from the private choice setting to a public choice setting. Privacy under two types of governments are characterized, authoritarian and democratic regimes. Privacy in the public domain is characterized by individual efforts at stealth (H) and signaling (S) and the detection efforts of government officials. Because of the nature of the programs administered by governments, some government officials may generally be friends in the sense that detection by them (or their agency) is associated with benefits, while others may be foes in the sense that detection by them (or their agency) may impose costs of the persons detected. To explore how governing institutions affect the likely mix of privacy-relevant policies, models of autocratic regimes of the leviathan type and of the perfect democratic of the median voter driven polities are developed. Intermediate forms of government are then modeled as convex combinations of these extremes.

A. Privacy in Autocratic Regimes: Leviathan

The first case analyzed is that of a leviathan government. Following Brennan and Buchanan (1977), it assumed that such governments maximize expected net revenue from its citizen-residents.[8] Assume that leviathan does not know the wealth or income of its

---

[7] Together the continuity and concavity assumptions are sufficient to assure that a Nash equilibrium exists. The large numbers of external effects imply that the overall equilibrium is unlikely to be Pareto efficient. Near universal demand for regulations that increase some forms of privacy implies that too little privacy often emerges from the Nash equilibrium, as with peeping-Tom laws, privacy regulations for financial institutions, and some forms of nuisance laws.

[8] Brennan and Buchanan (1977) and Olson (1993) are the pioneers in this literature. Olson points out that such a regime is likely to provide services that increase the net tax base. This possibility is

potential taxpayers, but can use direct and indirect detection methods to discover the tax base. The government knows that citizen taxpayers will attempt to avoid detection by agencies that impose losses, as in equation 3.1 above. Assume that the society of interest has M members and that leviathan imposes an average tax of amount L, when taxable wealth is discovered.

Expected net revenues given the tax avoiding (hiding) efforts of the citizenry in their dealings with an extractive government can be represented as:

$$R^e = M\, e(H^*, S^*, 1, D^E, t)\, L - g(D^E, t) \qquad (5)$$

where D^E 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^* is the average voter's effort at stealth (from equation 3.1), given the government's detection effort D^E and tax L. The cost of leviathan's detection efforts is $g(D^E, t)$.

For the purposes of the analytics, only the subset of taxpayer Nash equilibria in which the super-modularity condition holds are considered. This allows one to use the comparative statics of a typical taxpayer's best reply function to characterize changes in the overall Nash equilibrium.[9]

In such cases, net revenues are maximized when the leviathan's detection and tax rates satisfy:

$$ML(E_H H^*_{DE} + E_{DE}) - g_D = 0 \qquad (6.1)$$

$$ML(E_H H^*_L) + EM = 0 \qquad (6.2)$$

ignored here to characterize the worst possible form of government staffed by economic men and women. The extractive government is used to characterize a lower bound of government types.

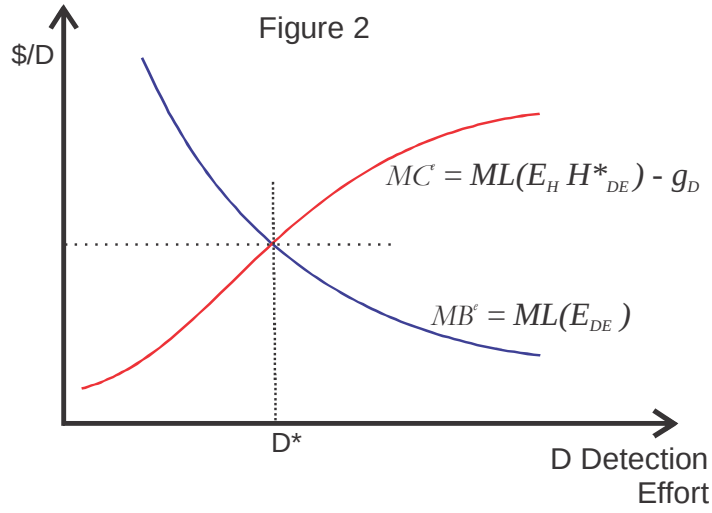
[9] See Amir (2005) for a useful survey of economic applications of the super-modularity concept. Many of the Nash equilibria that characterize economic contests have this property. That is to say, a change in game parameters induces qualitatively similar changes in the behavior of every player's best reply function and on the game's equilibria. This tends to be true, for example of most symmetric games.

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. Potential taxpayers hide rather than advertise their wealth in this setting, although they cannot hide it perfectly.

The government's marginal cost of detection includes two components, its direct marginal cost (g_D) and the indirect reduction in revenues generated by inducing greater effort to hide taxable income by those the detection efforts are deployed against ($MLE_H H^*_{DE}$). An increase in detection efforts tends to increase tax avoidance and thereby the size of the shadow economy. The optimal tax (L) equates the direct marginal revenue increase with its indirect reduction generated by increases in taxpayer avoidance efforts. It bears noting that detection efforts and taxes are both lower than they would have been without the avoidance efforts (stealth) by taxpayers.[10]

Figure 2 illustrates leviathan's optimal detection efforts in the Stackelberg equilibrium with private responses taken into account.

Figure 2



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.

[10] Possible 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.

$$D^* = d(M, L, t) \qquad (7.1)$$

$$H^* = h(0, L, 0, D^*, 0, 1, t) \qquad (7.2)$$

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

$$D^*_M = [(E_H H^*_D + E_D)L] / -[R^e_{DD}] > 0$$
if H effects are relatively small* (8.1)

$$D^*_L = [M(E_H H^*_D + E_D) + ML\, e_H H^*_{DL}] / -[R^e_{DD}] > 0$$
if H effects are relatively small.* (8.2)

$$D^*_t = M(E_{tH} H^*_D + E_H H^*_{tD} + E_{tD})L - g_{Dt} / -[R^e_{DD}] > 0$$
if H and cost effects are relatively small* (8.3)

The partial derivatives of Leviathan's detection efforts cannot be signed without making further assumptions about the extent to which citizens engage in efforts to hide their taxable wealth from the government.

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. An increase in average expropriation or fines (L) encourages greater detection efforts and greater stealth by taxpayers. 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 inframarginal effect of increased detection on revenue exceed the marginal cost of detection efforts and marginal reduction in the observed tax base from efforts to avoid detection.

Privacy in spheres of life in which leviathan has financial interests emerge as the joint outcome of government detection efforts and citizen efforts to hide their taxable wealth (H). Efforts to hide one's wealth are represented using equation 3.1, $H^* = h(0, L^*, 0, D^*, 0, 1, t)$.

The typical taxpayer is poorly served by leviathan in that taxes and secrecy are higher than ideal for most taxpayers.[11] Under the usual leviathan assumptions, few if any public services are provided from the taxes collected and so greater expenditures on stealth are induced than would have been the case if net benefits rather than net losses been conferred on citizens by the fiscal system.[12] The demand for privacy under revenue-maximizing governments induces a good deal of investment in hiding assets and income. The most tangible expression of such behavior is what many economists refer to as the underground economy.[13]

Exceptions to this corner solution in signaling ($S^*=0$) exist for those whose interactions with leviathan tend to be profitable. For example, successful rent seekers have less to fear and more to gain by being known to the rulers of authoritarian systems than a typical tax payer does. Such persons and organizations tend to behave as above for tax and regulatory purposes, where penalties rather than rents are at stake, but engage in considerable signaling to attract the attention of the persons in government in positions to confer rents.[14] A good deal of rent seeking behavior involves signaling so that one becomes known to the "right" people.

---

[11] The analysis focuses on the behavior of a typical taxpayer in the community of interest. If leviathan requires some minimal level of support to retain power, the government would provide benefits for the necessary subset of its residents. These beneficiaries of government largesse would regard government to be their friend, and therefore engage in signaling to receive benefits (gifts or rents) associated with their dictator's favor. A rational citizen's ideal combination of detection and conditional tax and grant programs, in principle, takes all such adjustments into account.

[12] If taxpayer responses are relatively large and effective, the signs of the above partial derivatives may be reversed. If increased government detection efforts are countered by increased efforts at stealth, as through earnings in a shadow economy, leviathan might rely upon other revenue sources to fund its activities. Congleton and Lee (2009) suggest that creating rent-seeking contests can provide an alternative to taxation, when taxes are difficult to collect. Such games induce signaling rather than stealth.

[13] Note that if tax avoidance (stealth, secrecy, or hiding) take the form of activities in the shadow economy, the above model can be used to characterize the size of the underground economy. All the factors that increase "stealth" tend to increase the size of the shadow economy.

[14] Rent-sharing as a means of retaining support sufficient to remain in power has been analyzed by Bueno de Mesquita, Smith, Silverson, and Morrow (2003) and North, Wallace and Weingast (2009). In such cases, leviathan should be regarded as a form of oligarchy rather than dictatorship, although the basic logic of the analysis in not significantly changed as long as the oligarchs share an interest in maximizing their net revenues.

Both the extent of the underground economy and corruption are both indicators of the demand for and production of privacy and fame in an authoritarian polity, although they involve quite different processes and behavior. In a complete leviathan model of fiscal policy, these are both determined at the margin by the choices of the autocrat or ruling coalition.

B. Privacy in Democratic Regimes

In contrast to a citizen's position under leviathan, the voter-citizens of a democracy often profit by calling attention to themselves in their dealings with government. Many government programs advance their interests, although a subset of those programs are normally designed so that benefits are available only to persons who "qualify." To obtain associated benefits, eligible citizens will attempt to become known to the official gatekeepers. They will stand in lines, fill out forms, send pictures, pay fees, answer questions, and so forth as necessary to "qualify" for the programs of interest.

However, this interest in becoming known does not characterize all relationships with a democratic government. In other cases, privacy rather than familiarity is the goal. Many tax and regulatory systems targeted rather than general, and both fines and tax obligations can often be reduced through various avoidance strategies. To avoid paying fines and taxes, citizens choose times and places for activities that make detection more difficult, rather than easier. One may drive faster than allowed on country roads rather than on city roads. Similar strategies can also be employed to avoid fines associated with violating waste-disposal rules or building codes. Tax liabilities can be hidden through cash transactions and the use of overseas banks. In such cases, stealth rather than signaling is likely to be employed by citizen-taxpayers.

Two majoritarian detection regimes are modeled below to illustrate the effects of technology on voter demands for privacy relevant policies of their governments. In principle, citizens what to be known by some parts and unknown by other parts of their governments. For the former, they will invest in signaling, and for the latter they will invest in hiding. The democratic government is assumed to produce unconditional (pure public goods) and conditional public services that are financed through a combination of

unconditional (unavoidable) and conditional (avoidable) taxes. The focus of analysis is again on privacy-relevant policies and behavior rather than the usual focus on fiscal policies, although fiscal policies are also modeled.[15]

Stove Pipes: Separate Detection Methods and Data

Let *G* be the level of a pure public good and B be the average benefit of being found eligible for a targeted program. The probability of being detected by a friend, F^*, is now interpreted as the probability that a person is found eligible for targeted benefit programs. The expected cost of the targeted benefit programs thus can be written as F^*MB, where M is the size of the community. The probability of being detected by an enemy, E^* is now interpreted as the probability of being found subject to an avoidable tax. If L is as the average penalty and tax collected, the expected revenue from this source is E^*ML in a community of size M. If the government operates under a balanced budget rule (or at close to its borrowing limit), the median voter's automatic tax payment, T^v, varies with his or her cost share, the cost of government services, and detection efforts net of conditional tax receipts collected.

Let γ be the government's cost function, and σ^v be the median voter's normal share of the net costs of government services. The median voter's ordinary tax obligation can be written as $\tau^{\varpi} = \sigma^v [\gamma - E^*ML] = \sigma^v [\gamma(F^*MB + G, D^F, D^E, t) - E^*ML]$, where cost function γ includes production costs, detection costs, D^F and D^E, and the effects of technology, t. The median voter's expected net benefits from government are determined by his or her

[15] There is a large public finance literature on tax evasion and tax avoidance that focuses for the most part taxpayer behavior within Western democracies. Tax evasion and avoidance are for the most part analyzed as a law and economics problem or public finance problem rather than an aspect of political economy. See for example, Slemrod and Ytzhaki (2002) or Feldstein (1999). There is also a large accounting literature on legal strategies for minimizing tax payments and for detecting illegal forms of tax avoidance, which increase risks for investors. See, for example, Desai and Dharmapala (2006) for a model of how and empirical evidence that corporate reward systems affect corporate (managerial) tax avoidance strategies and stock market responses to those strategies. The analysis of this section focuses on the codetermination of detection and evasion strategies. Most other studies assume that detection strategies are exogenous or set by benevolent central planners. It also differs from the usual public finance analysis by focusing on the effects of government detection and voter hiding and signaling on privacy, rather than the fiscal aspects of tax and expenditure regimes.

own expected benefits and costs from government services, and his or her expenditures on stealth and signaling.

$$N^e = v(G) + f(H^*, S^*, D^F, t)B - c(H^*, S^*) - e(H^*, S^*, D^E, t)L$$
$$- \sigma^v [\gamma(f(H^*, S^*, D^F, t)MB + G, D^F, D^E, t)) - e(H^*, S^*, D^E, t)ML] \quad ((9)$$

where $V = v(G)$ is the benefit (reservation price) from the pure public good for the median voter, f^*B is the expected value of conditional benefits, c is the cost of hiding and signaling, e^*L is the expected cost of conditional fines, and $\sigma^v [\gamma - E^*ML]$ is the median voter's associated broad-based tax payment. Note that equation 9 includes the median voter's best-reply functions for stealth and hiding characterized above as arguments. 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*).

Suppose that the government uses separate detection regimes for its tax collection, D^E, and benefit conferring programs, D^F. The median voter's ideal vector of the pure public good (G), targeted benefit programs (B), detection efforts (D^E and D^F), and tax avoidance penalties (L) satisfy:

$$N^e_G = V_G - \sigma^v [\gamma_G] = 0 \quad (10.1)$$

$$N^e_{DF} = F_{DE}B + (BF_H - C_H)H^*_{DF} + (BF_S - C_S)S^*_{DF}$$
$$- \sigma^v [g_G F_H MB + g_{DF} - E_H ML] (F^*_{DF} + S^*_{DF}) = 0 \quad (10.2)$$

$$N^e_{DE} = -E_{DE}L + (LE_H - C_H)H^*_{DE} + (LE_S - C_S)S^*_{DE}$$
$$- s^v [MBg_G F^*_{DE} + g_{DE} - E^*_{DE} ML](F^*_{DE} + S^*_{DE}) = 0 \quad (10.3)$$

$$N^e_B = F - \sigma^v [\gamma_G(FM)] + (F_H H^*_B + F_S S^*_B)B - (E_H H^*_B + E_S S^*_B)L$$
$$\sigma^v [\gamma_G(F_H H^*_B + F_S S^*_B)MB] - (C_H H^*_B + C_S S^*_B) = 0 \quad (10.4)$$

$$N^e_L = -E - \sigma^v [EM] + (F_H H^*_L + F_S S^*_L)B - (E_H H^*_L + E_S S^*_L)L$$
$$- \sigma^v [(E_H H^*_L + E_S S^*_L)ML] - (C_H H^*_L + C_S S^*_L) = 0 \quad (10.5)$$

The entire system of equations holds simultaneously at the median voter's multidimensional ideal point. There are a wide range of complex interactions and tradeoffs that need to be accounted for in even a relatively lean model of privacy-relevant government policies.[16]

A good deal of insight can be obtained by considering each of the first order conditions separately. 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 from the public good (U_G) equal to her share of the marginal costs of providing it ($s^v [g_G]$).

The other first order conditions are more complex, because each of these policy instruments induces avoidance and signaling responses by the median voter (and other citizens). Partial derivatives of H* and S* are from equation 4.5 and its signaling counterpart. The comparative static results developed in the first section of the paper imply that an increase in targeted benefit programs or efforts to find persons eligible for such programs induces an increase in citizen signaling behavior and a decrease in stealth efforts. When benefits are large, signaling will be high, and detection efforts can be low. Privacy falls as conditional benefits increase, other things being equal.[17]

Changes in tax avoidance penalties and detection rates have similar but opposite effects on signaling and stealth efforts. An increase in conditional benefits tends to increase signaling behavior and reduce privacy. An increase in taxes tends to increase stealth and privacy other things being equal. However, these effects are at least partly offset by changes in a government's detection policies.

Changes in technology that increase the effectiveness of detection allow the same revenue to be collected with lower tax rates, other things being equal. Privacy tends to fall, both because detection avoiding strategies become less effective and so are less used, while the government's detection efforts tend to increase insofar as the cost of detection falls.

---

[16] 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.

[17] Part of the signaling costs in this case may be waiting in long lines to reach the persons who decide whether one "qualifies" or not for a conditional benefit program.

Big Data: Integrated Detection Methods

In the above setting, detection and information gathering for conditional tax and benefit programs are assumed to be two separate systems, with an effective "firewall" between them. The information collected from system E is used for a single purpose, tax collection. The information collected through system F is exclusively used to award benefits. Such data partitions are less common today, because of recent innovations in software for combining records and reductions in the cost of data storage, integration, and mining—what has been called "big data."

With the advent of the "big data" technologies, all detection efforts become part of one unified recognition and information processing system. The shift to "big data" technology unsettles the previous political (and private) equilibria with respect to privacy in a manner that differs from improved detection technologies, because it creates a new link between the probabilities of being detected by "friends and foes" in government.

This can be demonstrated by modifying the previous model to account for big data by replacing D^E and D^F in the above model with a single detection level, D. The median voter's expected net benefit equation becomes:

$$N^e = f(H^*, S^*, D, t)B - e(H^*, S^*, D, t)L - c(H^*, S^*) + u(G) - \sigma^v [\gamma(F^*MB + G, D, D, t)) - EML] \quad (11)$$

Her ideal level of government detection effort now satisfies:

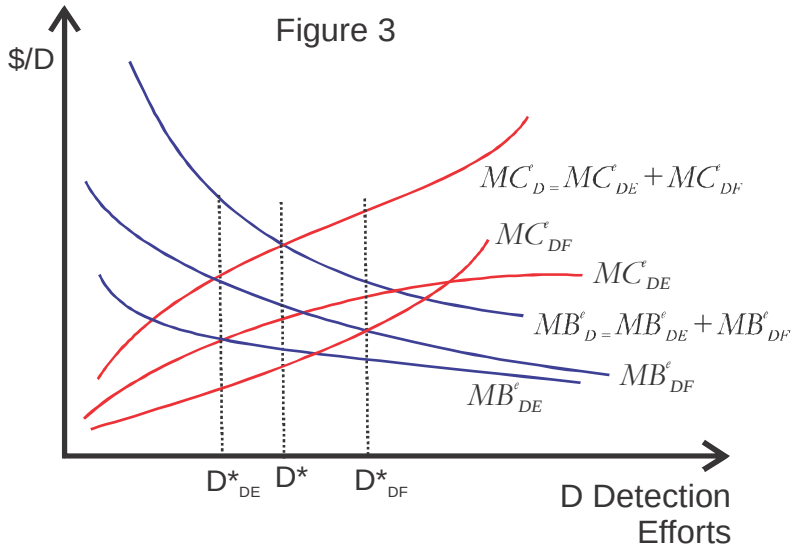
$$N^e_D = F_{DF}B - \sigma^v [\gamma_D] + (BF_H - C_H)H^*_{DF} + (BF_S - C_S)S^*_{DF} - E_{DE}L - \sigma^v [\gamma_D - E_D ML] + (LE_H - C_H)H^*_{DE} + (LE_S - C_S)S^*_{DE} = 0 \quad (12)$$

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

Insofar as the equilibrium in the previous choice implied higher detection efforts for distributing benefits than for collecting taxes, $D^F > D^E$, the new first order condition implies a somewhat smaller detection effort for handing out benefits and a higher rate for

detecting tax avoidance. The new optimal detection rate tends to be between those levels, and ($D^* < D^F + D^E$), as illustrated in figure 3. The sum of the "stove pipe" marginal cost and marginal benefit curves characterize the "big data" detection system, which implies an ideal detection effort between the original ones. This new optimal single effort level is clearly less costly than the sum of the previous separate effort levels. (It is on the order of half as much as previously spent in Figure 3.) Fewer resources, not more, should therefore be invested in detection regimes under a big data than under a stove pipe regime.

Recent voter, interest group, and mass media concerns about privacy invasions by democratic governments are consistent with this result.



IV. Some Interpolations: Between Leviathan and Democracy

In between a well-functioning majoritarian states and leviathan are a variety of intermediate government types in which groups of various sizes "capture" the machinery of governance and use it to advance their own agendas. These systems are often presumed to choose policies between those demanded by autocracies and democracies, although we have no good models of these intermediate forms of government.

Intermediate outcomes may occur, for example, when government policies advance the interest of ruling coalitions that include less than half the population of voters but more than a single person. The interests of persons in a minority government tend to have general interest that are similar to those of the typical voter-taxpayer, but may target less than

general taxes at persons outside government while concentrating the benefits of conditional government programs within the ruling minority coalition. In such cases, the policies chosen tend to lie between those of majority rule and leviathan.[18]

If so, the results of the previous three sections can be used to analyze the continuum of government types between democracy and leviathan. Ignoring differences in citizen responses to detection efforts because of tax-morale effects, tax-related detection levels tend to increase as one shifts from majority rule towards minority rule, as is indicated by equations 6 and 10.3. Under leviathan, tax avoidance detection efforts satisfy:

$$M\,(E_H\,H^*_{DE} + E_{DE}\,)L - g_D = 0 \qquad (13.1)$$

Under majority rule it satisfies:

$$-E_{DE}L + (LE_H - C_H)H^*_{DE} + (LE_S - C_S)S^*_{DE}$$
$$- s^v\,[MBg_G F^*_{DE} + g_{DE} - E^*_{DE}\,ML](F^*_{DE} + S^*_{DE}) = 0 \qquad (13.2)$$

The main difference between these two expressions is that the median voter takes account of direct effects of the privacy policies on herself: her possible tax penalties, her stealth and signaling efforts and costs (the top line of 13.2). The terms in the second line (after s^v) are ones associated with net revenue effects including effects on conditional benefit programs and revenues. Were it not for the additional terms associated with personal effects, the first order conditions for tax-related detection efforts would be very similar to leviathan's.

These terms imply that the marginal costs of government detection efforts tend to be higher for a median voter than for leviathan, even in the case in which the penalties collected are of the same magnitude (L). Leviathan is untaxed and so does not increase its stealth in response to higher tax rates.[19] In intermediate forms of governments, the result is

[18] A ruling minority's policies may also differ from those of a majority if the persons included are in unrepresentative of the citizenry as a whole. They might, for example, be richer than the median voter or less risk averse. The effects of different types of pivotal voters are beyond the scope of the present analysis.

[19] Audit rates in democracies tend to be quite small (Congleton 2002). The survey evidence explored in Feld and Larsen (2012), for example, suggests that tax avoidance problems would be a reason for voters to prefer less than complete review of tax returns. Their work also suggests that it is tax morale or honesty, rather than detection rates, that accounts for the relatively high yields of Western tax systems.

modeled as a convex combination of the two optimizations, and the result tends to be in between, moving closer and closer to leviathan as the median voter loses influence relative to narrow rent-seeking interests.

This effect is likely to be reinforced by changes in the tax system. If the amount collected through targeted taxation and fines increase as the regime types shift toward leviathan (e.g. L increases as one moves from majority rule towards leviathan) the marginal benefit of detection efforts for the pivotal voters of the ruling coalition increase relative to that of the median voter. Thus, detection efforts tend to rise as regime-types move toward leviathan.

As a consequence privacy in the tax and regulatory domains tends to fall, as regime types shift from democracy to autocracy, other things being equal.

V. Conclusions

This paper has begun the task of modeling the personal demand for privacy and its effects on public policy. To do so required a framework general enough to address the questions, yet simple enough to be mathematically tractable and yield plausible results. As modeled, privacy is not a deterministic good that directly generates utility or net benefits, but rather a stochastic variable that is desired because of its likely consequences—consequences that vary with circumstances. In some settings, privacy improves a person's well-being by reducing the probability of being subjected to losses from others in the community. In others, privacy reduces a person's well-being by reducing the probability of realizing benefits associated with being recognized.

The analysis of public policies relevant to privacy noted that citizen tax payers often simultaneously undertake signaling and stealth with respect to governments and government officials. To illustrate the range of tradeoffs that voters confront when voting on such policies, a lean model of government policy making was introduced in which governments create both general and targeted benefits financed from taxes that combine general and conditional taxation. The focus of analysis was not the fiscal package, but rather effects of such systems on the pattern of private relevant behavior between governments and citizens.

In general citizens want less privacy with respect to targeted benefit programs than with respect to targeted tax programs. This affects their own behavior and the pattern of detection efforts they favor from government officials. The framework and models developed are sufficiently general that they be readily extended to analyze other areas of policy as in with health services, law enforcement, and national security (counterespionage and anti-terrorism efforts). The results are likely to be broadly similar to those developed above.

Both the leviathan and the median voter models demonstrate that tax and expenditure policies have complex effects on taxpayer demands for privacy. Facing a revenue maximizing government of the Brennen and Buchanan variety, ordinary taxpayers would tend to be relatively stealthy and secretive with respect to government, because there are mainly costs associated with being detected by such governments. Leviathan nation states thus tend to have relatively large underground economies, as is consistent with empirical evidence. Under majority-rule based governance, the analysis implies that citizen-voters will tend to engage in a mix of hiding and signaling strategies. Signaling is used to qualify for conditional benefits and stealth to avoid conditional forms of taxation and penalties.

Voter support for government detection efforts varies among policy areas, with a demand for greater detection efforts by governments in policy areas in which voter expect benefits, and lesser ones in cases in which he or she expects to be subject to costs. Technology also affects the tradeoffs the voters must take account of. For example, a shift to "big data" affects both the public and private equilibria with respect to detection, stealth, and signalling. Voters generally favor a reduction in information gathering expenditures as data bases are combined, other things being equal.

The analysis also indirectly suggests that restrictions on government intrusiveness can make sense from utilitarian and contractarian perspectives, insofar as governments may occasionally be captured by minority factions that maximize their own relatively narrow benefits, rather than advance majority interests. A leviathan whose detection efforts could be constitutionally constrained would be more attractive to live under, than one whose efforts to collect taxes and detect avoidance are constrained only by its economic interests.

References

Amir, R. (2005) "Supermodularity and Complementarity in Economics: An Elementary Survey," *Southern Economic Journal* 71: 636-60.

Brennan G., and Buchanan, J. M. (1977) "Toward a Tax Constitution for Leviathan," *Journal of Public Economics* 8: 255-73.

Buchanan, J. M. and Tullock, G. (1962) *Calculus of Consent*. Ann Arbor: University of Michigan Press.

Bueno de Mesquita, B., Smith, A., Siverson, R. M., and Morrow, J. D. (2003) *The Logic of Political Survival*. Cambridge: MIT Press.

Congleton, R. D. (2002) "Risk-Averse Taxpayers and the Allocation of Tax Enforcement Effort: Law Enforcement or Leviathan? Some Empirical Evidence," *Public Finance Review* 30: 456-476.

Congleton, R. D. and Lee, S. (2009) "Efficient Mercantilism? Revenue-Maximizing Monopolization Policies as Ramsey Taxation," *European Journal of Political Economy* 25 (2009): 102-14.

Cowen, T. (2000) *What Price Fame?* Cambridge: Harvard University Press.

Desai, M. A. and Dharmapala, D. (2006) "Coporate tax Avoidance and High-Powered Incentives," *Journal of Financial Economics* 79: 145-79.

Feld, L. P. and Larsen, C. (2012) *Undeclared Work, Deterrence and Social Norms: the Case of Germany*. Heidelberg: Springer.

Feldstein, M. (1999) "Tax Avoidance and the Deadweight Loss of the Income Tax," *Review of Economics and Statistics* 81: 674-80.

Kuran, T. (1995) *Private Truths, Public Lies: The Social Consequences of Preference Falsification*. Cambridge Mass: Harvard University Press.

North, D. C, Wallace, J. J. and Weingast, B. R. (2009) *Violence and Social Orders*. Cambridge: Cambridge University Press.

Olson, M. (1993) "Dictatorship, Democracy, and Development," *American Political Science Review* 87: 567-76.

Posner, R. A. (1981) "The Economics of Privacy," *American Economic Review* 71: 405-09.

Posner, R. A. (1979) "Privacy, Secrecy, and Reputation," *Buffalo Law Review* 28:1-55.

Plott, C. R. (1967) "A Notion of Equilibrium and its possibility under Majority Rule," *American Economic Review* 57: 787-806.

Schneider, F. and Enste, D. (2000) "Shadow Economies Around the World: Size, Causes, and Consequences," IMF Working Paper.

Slemrod, J. and Yitzhaki, S. (2002) "Tax Avoidance, Evasion, and Administration," *Handbook of Public Economics*. Amsterdam: Elsevier, pp. 1423-1470.

Moore, A.D. (2010) *Privacy Rights, Moral and Legal Foundations*. University Park, PA: Pennsylvania State University Press.

Vanberg, V. and Buchanan, J. M. (1989) "Interests and Theories in Constitutional Choice," *Journal of Theoretical Politics* 1: 49-62.