On the Political Economy of Privacy in Communities that Include Both Friends and Foes[1]

Roger D. Congleton
Dept. of Economics
West Virginia University

roger.congleton@mail.wvu.edu

7-9-18

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.

JEL Categories: D71, D6, D8

[1] I would like to thank the editors and a referee for helpful suggestions and for overlooking several typos on the first drafts of the paper submitted to the journal. I would also like to thank the founding editor of this journal, Domenico D'Empoli, for his support over many years and wish the new editors continued success.

I. Introduction: On the Nature of Privacy and Fame

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. His or her privacy and fame are joint products of that person's decision to walk through the village in a particular manner and of the decisions of others to watch and remember what they observed. Such natural reductions in privacy occur without technological support.[2]

Such "invasions" of privacy are consequences of the evolution of sight organs and nervous systems. Sight, hearing, smell, and memory have obvious survival advantages, in part because they reduce the privacy of others, making both friends and foes easier to identify. Privacy also has survival advantages. It makes one less likely to be eaten for lunch or otherwise taken advantage of. Evolution thus also supports both detection and privacy generating capacities. To counter the effects of eyes and ears, many species have camouflage coloring, the capacity for near silent movement, and strategies for using night and shadow as times to move or sleep. To counter those efforts to avoid detection, many predators have acute detection systems that include night vision, hearing, smell, and "data processing" skills.

Natural methods of increasing privacy are thus nearly always incomplete. Even a stealthy walk through a village may be observed by others even in dim light. A stealthy person is visible, makes a bit of noise, and leaves a detectable odor. Such losses of privacy occur partly because of the survival advantages of countervailing detection abilities.

[2] 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.

However, others are products of intent. Many persons desire to be seen or heard by persons who are friends or at least not enemies. 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 such 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. One may walk and dress in a manner to attract the attention of those watching.

In human societies, biological tradeoffs are compounded by risks associated with a variety of conflicts and complementarities associated with life in organizations and communities. On the one hand, secrecy often reduces conflict and increases the likelihood of success by generating useful informational asymmetries.[3] On the other, there are circumstances in which a bit of fame is helpful. Many sellers of goods and services position themselves at prominent places within their communities to attract attention to the goods they offer for sale.[4] Attracting attention to oneself makes mutually beneficial relationships more likely to develop, at the same time that it increases risks from rivals and predators.

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. Many of the tradeoffs involved can be clarified with a rational choice model of stealth and signaling strategies and the rewards from each. Section II models the private tradeoffs between stealth and signaling. Section III uses the model to analyze government policies that attempt to reduce the effectiveness of stealthy strategies and/or to 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. Changes in technology, such as "big data," affect voter support for public investments in privacy reducing services.

[3] 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.

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

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 are observed by others. The second reduces privacy by increasing the probability that the activity of interest is noticed by others.[5] 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) always produces losses. Typical benefits from finding friends are denoted B, with B≥0. Typical losses imposed by foes are denoted L, with L≥0.

The probability that the 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 differing numbers. The probability of being noticed by a friend can be represented as: $F = f(H, S, N^F, D^F, t)$, where H is the individual of interest's effort at hiding and S is his or effort at signaling, N^F is the number of friends, D^F is their average effort at detection, and t is the technology available to each. Similarly, the probability of being noticed by an enemy can be represented as $E = e(H, S, N^E, D^E, t)$.

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 for all one's activities, 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.

One's overall 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. Similar F and E functions exist for every activity that one might engage in,

[5] 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.

and each would have its own *H, S, D^F, D^E, N^F,* and *N^E*. One might want some activities to be known and others private. One's overall privacy or fame would be the sum across all activities. There is a vector of privacy and fame levels among one's activities.

However, to simplify the exposition, only a single activity is focused on. Focusing on one activity at a time allows one to examine the tradeoffs that affect choices with respect to a "typical" activity, which in turn characterize how efforts at hiding and signally vary among the many activities one may undertake. This would be the case when the privacy associated with each person's many activities is determined independently of the others.

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. 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.

[Figure 1 around here]

The implicit function theorem allows the optimal combination of stealth and signaling for the activity of interest 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 for the activity of interest.[6]

Note that privacy is only partly controlled by the individual. It is generated jointly by that individual'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:

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

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

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

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

[6] 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.

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 also 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. The partial derivatives 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) decreases 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 increases 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.[7]

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 absolute, and persons may simultaneously engage in behavior that increases and diminishes overall 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 jointly emerge from the decisions of all persons in a community, which 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.[8]

III. The Political Economy of Privacy

We now shift from the private choice setting to a public choice setting. Privacy under several types of governments are characterized in this section: authoritarian, democratic, and those in between. Privacy in the public domain is characterized by individual efforts at

[7] 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.

[8] 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. Moreover, there may too little fame in some areas of life and too little privacy in others. Most economists, for example, would like to be a bit more famous than they are.

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 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 on 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 type (where all policies are median voter driven) of polities are developed below. Intermediate forms of government are then modeled as convex combinations of those 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 their citizen-residents.[9] Assume that leviathan does not know the wealth or income of its individual 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 it tax collectors, as in equation 3.1 above. Assume that the society of interest has *M* members and that leviathan imposes an average tax levy 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 and indirect efforts to estimate wealth or income by census counts, indicators of 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 $g(D^E, t)$.

[9] 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 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.

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.[10]

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

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

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

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 the 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 (hiding/stealth) by taxpayers.[11]

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

[10] 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.

[11] 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.

[Figure 2 around here]

The implicit function theorem allows leviathan's optimal detection and tax rates to be represented as functions of national population, the average revenue recovered, and the state of detection technology.

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

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

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

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

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

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

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. Assumptions about the relative magnitudes of the effects are necessary.

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 both 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 over at least part of the range of interest.

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, with H* = h(0, L^*, 0, D^*, 0, 1, t).

The typical taxpayer is poorly served by leviathan in that taxes and detection efforts are higher than ideal for most taxpayers.[12] Under the usual leviathan assumptions, few if any public services are provided from the taxes collected and tax avoidance is greater than would have been the case if net benefits rather than net losses been conferred on citizens by the fiscal system.[13] The most tangible expression of such behavior is what many economists refer to as the underground economy and also the numerous banks in tax havens.[14]

Exceptions to this corner solution in signaling (S*=0) exist for those whose interactions with leviathan tend to be profitable. For example, 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

[12] 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.

[13] 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.

[14] 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. See Schneider and Enste (2013) for an extensive survey of empirical evidence on the size and distribution of shadow economies around the world.

to attract the attention of the persons in government that have the authority to confer rents.[15]

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, given the anticipated responses of taxpayers and rent seekers.

B. Privacy in Democratic Regimes

In contrast to a citizen's position under leviathan, many of the voter-citizens of a democracy profit by calling attention to themselves in their dealings with government. Many government programs are conditional and are avaible only to those who qualify in one way or another. To obtain associated benefits, eligible citizens 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 are 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. Tax liabilities can be hidden through cash transactions, clever accountants, and the use of overseas banks. 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 building codes or waste-disposal rules. In such areas of life, stealth rather than signaling is likely to be employed by pragmatic citizen-taxpayers.

[15] A good deal of rent-seeking behavior involves signaling so that one becomes known to the "right" people. 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.

In general, pragmatic citizens want 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.

Two majoritarian detection regimes are modeled below to illustrate the effects of technology on voter demands for privacy. The model includes one policy in which fame or familiarity is sought and another in which privacy or anonymity is sought. The 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 on privacy-relevant policies (median voter preferences over detection efforts) rather than on fiscal policies, although fiscal policies are also modeled.[16]

Stove Pipes: Separate Detection Methods for Services and Taxes

Let G be the level of a pure public good and B be the average benefit of being found eligible for an associated conditional program of public services. The probability of being detected by a friend, F^*, is now interpreted as the probability that a person is found eligible for a conditional benefit program. The expected cost of the targeted benefit program(s) thus can be written as F^*MB, where M is the size of the community.

The tax system used to finance the public and conditional services is assumed combine unconditional and conditional tax payments. The probability of being detected by an enemy, E^* is now interpreted as the probability of being found subject to a potentially avoidable tax. If L is as the average penalty and tax collected from the conditional tax, the

[16] 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.

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

$$\begin{aligned} N^{e} = {} & v(G) + f(H^{*}, S^{*}, D^{F}, t)B - c(H^{*}, S^{*}) - e(H^{*}, S^{*}, D^{E}, t)L \\ & - \sigma^{v} [\gamma(f(H^{*}, S^{*}, D^{F}, t) MB + G, D^{F}, D^{E}, t)) - e(H^{*}, S^{*}, D^{E}, t) ML] \qquad ((9) \end{aligned}$$

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:

$$N^{e}{}_{G} = V_{G} - \sigma^{v} [\gamma_{G}] = 0 \qquad (10.1)$$

$$\begin{aligned} N^{e}{}_{DF} = {} & F_{DE}B + (BF_{H} - C_{H})H^{*}{}_{DF} + (BF_{S} - C_{S})S^{*}{}_{DF} \\ & - \sigma^{v} [g_{G}F_{H} MB + g_{DF} - E_{H} ML] (F^{*}{}_{DF} + S^{*}{}_{DF}) = 0 \qquad (10.2) \end{aligned}$$

$$\begin{aligned} N^e{}_{DE} = -E_{DE}L + (LE_H - C_H)H^*{}_{DE} + (LE_S - C_S)S^*{}_{DE} \\ - s^{\,v}\,[MBg_GF^*{}_{DE}+g_{DE} - E^*{}_{DE}\,ML](F^*{}_{DE} + S^*{}_{DE}) = 0 \end{aligned} \qquad (10.3)$$

$$\begin{aligned} N^e{}_B = F - \sigma^v\,[\gamma_G(FM)] + (F_H\,H^*{}_B + F_SS^*{}_B)B - (E_H\,H^*{}_B + E_SS^*{}_B)L \\ \sigma^v\,[\gamma_G(F_HH^*{}_B + F_SS^*{}_B)MB] - (C_HH^*{}_B + C_SS^*{}_B) = 0 \end{aligned} \qquad (10.4)$$

$$\begin{aligned} N^e{}_L = -E - \sigma^v\,[EM] + (F_H\,H^*{}_L + F_SS^*{}_L)B - (E_H\,H^*{}_L + E_SS^*{}_L)L \\ -\sigma^v\,[(E_H\,H^*{}_L + E_SS^*{}_L)ML] - (C_HH^*{}_L + C_SS^*{}_L) = 0 \end{aligned} \qquad (10.5)$$

The entire system of equations holds simultaneously at the median voter's multidimensional ideal point.[17]

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 democratic policies.
A good deal of insight concerning the median voter's ideal combination can be obtained by examining each of the first order conditions separately. Doing so, in effect holds the other control variables constant, and is intended to provide some intuition about the implications of the first order conditions. 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 his or her marginal cost 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 with respect to conditional

[17] 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. Alternatively, institutions may, for example, separate the decisions so that the median voter equilibrium emerges as the median ideal point in each dimension of policy, taken one at a time. A full equilibrium in the latter case will also satisfy all 5 first order conditions.

benefit programs can be low. Privacy with respect to the activities that produce conditional benefits fall as conditional benefits increase, because of increased signaling, rather than governmental detection efforts, other things being equal.[18]

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 partly offset by changes in a government's detection policies with respect to conditional taxes. Privacy is likely to fall as conditional taxes increase, because of increased detection efforts by the government, rather than signaling.[19]

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.

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

[18] 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.

[19] This assumes that governments are more effective at detection than citizens are at tax avoidance (hiding). In cases in which governments are ineffective at detection, privacy may increase as the conditional activities are shifted to the underground economy or tax havens.

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:

$$\begin{aligned} N^e = f(H^*, S^*, D, t)B - e(H^*, S^*, D, t)L - \mathrm{c}(\mathrm{H}^*, \mathrm{S}^*) + u(G) \\ - \sigma^v [\gamma(F^*MB + G, D, D, t)) - EML] \end{aligned} \qquad (11)$$

Her ideal level of government detection effort now satisfies:

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

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. Those sums imply an ideal detection effort between the original ones. (It is on the order of half as much as previously spent as illustrated in Figure 3.) Fewer resources, not more, should therefore be invested in detection regimes under a big data than under a stove pipe regime.

[Figure 3 around here]

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 governmental 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. What might be called "minority governments" can be thought of in terms of reduced suffrage, which systematically excludes many or most citizens from voting, or as simply the effects of "political elites" of various sizes. In principle, such ruling juntas may range from two persons to ones that include most of the citizenry.

The persons in a relatively inclusive government, tend to have interests that are similar to those of the typical or median voter-taxpayer, but as the number of voters declines they more and more resemble leviathan who can target taxes at persons outside government, while concentrating the benefits of conditional government programs within the ruling coalition. For such governments, the policies chosen tend to lie between those of majority rule and leviathan.[20]

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:

$$-E_{DE}L + (LE_H \;\; - C_H)H^*_{DE} + (LE_S - C_S)S^*_{DE}$$

[20] European advocates of expanded suffrage in the late nineteenth and early twentieth century, such as Wicksell and Puviani thought that taxing the unrepresented was serious policy problem, one that led to the use of less than efficient tax systems and provided services that were not linked to tax payments.

$$-s^{v}\,[MBg_{G}F^{*}_{DE}+g_{DE}-E^{*}_{DE}\,ML](F^{*}_{DE}+S^{*}_{DE})=0 \qquad (13.2)$$

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). However, as modelled here, Leviathan is untaxed and so does not increase its stealth in response to higher tax rates.[21] In intermediate forms of governments, public policies can be modelled as a convex combination of the two policy extremes. Such a characterization—which is similar to that used in empirical work with various democracy indices (such as the Polity index)—implies that the policies of minority governments tends to be in between the median voter and leviathan outcomes. The outcomes move toward leviathan as the median voter loses influence.

This interest effect on policy is likely to be reinforced by changes in the tax and benefit systems. As the amount collected through taxation and fines increase on persons outside the ruling coalition increase and benefits tend to be concentrated on persons inside the ruling coalition, tax payer responses more and more closely resembles that under leviathan (e.g. L increases and B decreases 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 to the extent that the new conditional programs favor the ruling minority. Both effects imply that detection efforts tend to rise as regime-types move toward leviathan.

[21] 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 suggests that it is tax morale or honesty, rather than detection rates, that accounts for the relatively high yields of Western tax systems.

Privacy in the tax and regulatory domains thus tends to fall for citizens outside government, as regime types shift from democracy to autocracy, assuming that the various forms of government are equally effective at collecting taxes and producing services.

V. Conclusions

This paper has begun the task of modeling the personal demand for privacy and its effects on public policy. To do so, it has developed a framework general enough to address the questions, yet simple enough to be mathematically tractable and yield plausible results. The framework shows how privacy policies and ordinary public policies are connected, how privacy demands vary across policies, and how technology affects citizen demands for privacy. As tends to be true of any reasonably general model, the conclusions reached depend on assumptions about the relative size of a several partial derivatives. For the purposes of the narrative, several mathematical assumptions were made to sharpen the conclusions reached. In general, they were ones that produced results that are consistent with economic intuitions, which in turn tend to require separability of key functions or low levels of interdependence among variables (zero or small cross partials). The ambiguity of the model without such restrictions implies that empirical work will ultimately be necessary to determine whether these assumptions shed useful light on the demand functions characterized by the model.

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. With respect to public policies, most persons want little privacy in areas in which benefits are conditioned on being known, but want a good deal privacy in areas in which taxes, fines, and fees are conditioned on being known. As a consequence, citizen tax payers often simultaneously undertake signaling and stealth with respect to governments and government officials.

The analysis used public finance policies to illustrate both responses to government policies and demands for them. The main focus was not the fiscal package, but rather effects of such systems on the pattern of private relevant behavior between governments and citizens. The framework is sufficiently general that it can be readily extended to other areas of policy as in with health services, law enforcement, economic regulation, and national security (counterespionage and anti-terrorism efforts). The results are likely to be broadly similar to those developed above.

The leviathan and the median voter models demonstrate that political institutions have systematic effects on 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. The analysis thus predicts that leviathan nation states tend to have relatively large underground economies, which 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 systematically among policy areas and with technological innovations. There is a greater demand for detection efforts by governments in policy areas in which voters expect benefits, and lesser ones in areas in which he or she expects to be subject to costs. Technology also affects the tradeoffs the voters must take account of. Recent innovations in "big data" affects both the public and private equilibria with respect to detection, stealth, and signaling. Voters generally favor a reduction in information gathering expenditures as data bases are combined, other things being equal. The European Union's recent change in rules with respect to privacy are consistent with this prediction.

The analysis also indirectly provides support for constitutional restrictions on government intrusiveness. Such restrictions are supported by utilitarian and contractarian normative theories, whenever it is possible that governments are occasionally captured by minority factions that maximize their own relatively narrow benefits, rather than advance majority interests. Constitutional provisions that restrict a governments ability to search through a person's personal possessions—such as the fourth amendment to the constitution of the United States—are consistent with this normative conclusion. Similarly, a leviathan whose detection efforts are 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) 'Corporate 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. (2013) *The shadow economy: An international survey.* Cambridge UK: Cambridge University Press.

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.

Figure 1: The demand for privacy and fame

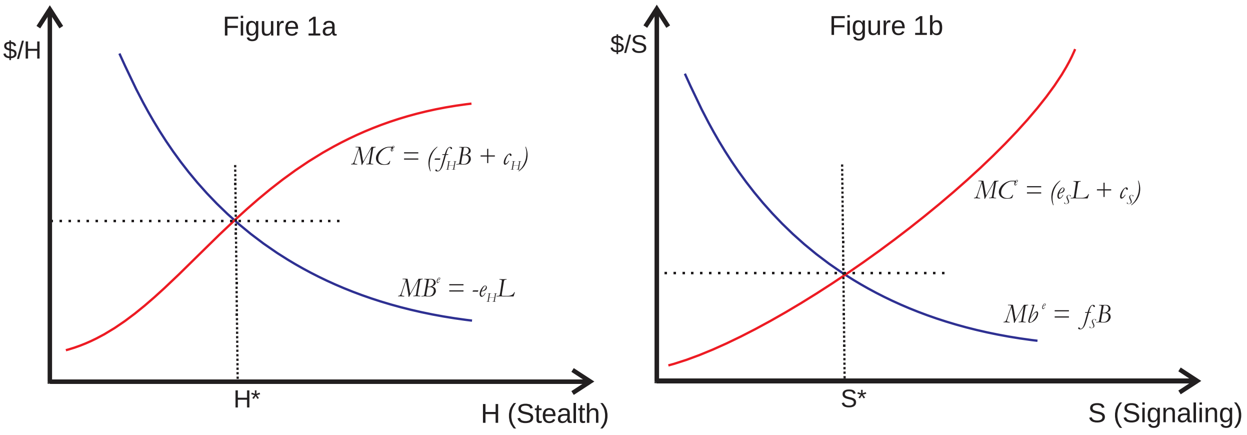


Figure 2: Leviathan’s Optimal Detection Effort

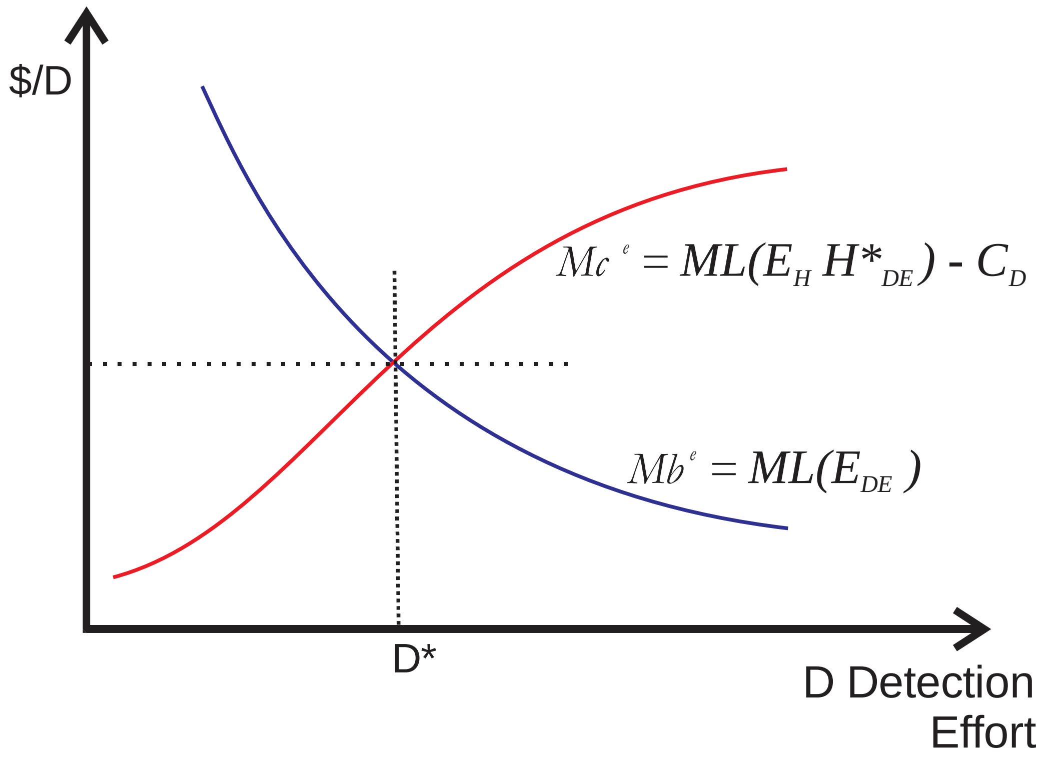
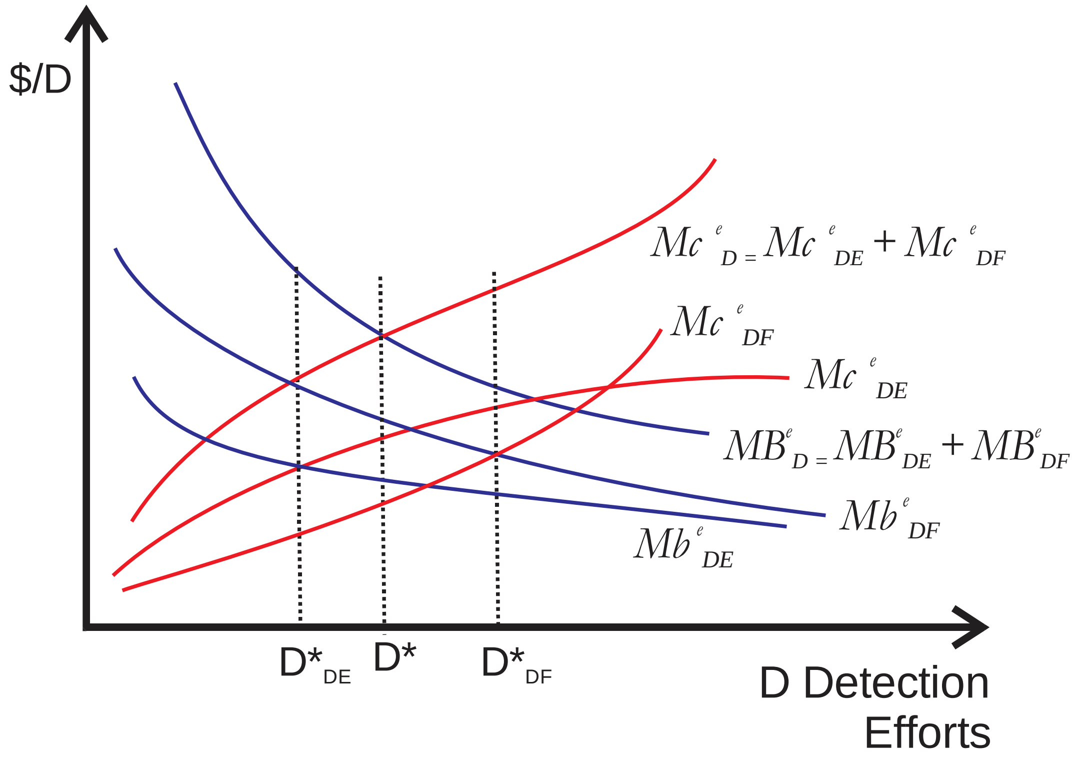


Figure 3: Effect of Technological Adance (Big Data) On Median Voter Demands for Detection


$/D
$Mc^{e}_{D} = Mc^{e}_{DE} + Mc^{e}_{DF}$
Mc^{e}_{DF}
Mc^{e}_{DE}
$MB^{e}_{D} = MB^{e}_{DE} + MB^{e}_{DF}$
Mb^{e}_{DF}
Mb^{e}_{DE}
D^{*}_{DE}
D^{*}
D^{*}_{DF}
D Detection
Efforts