Privacy, Polarization, and Passage of Divisive Laws

Benjamin Johnson[1] and Paul Laskowski[2]

[1] No Affiliation
benjaminejohnson@gmail.com
[2] UC Berkeley
paul@ischool.berkeley.edu

Abstract. Notions of privacy are particularly salient to marginalized groups of people, especially when they find themselves disproportionately affected by the enforcement of laws. We use game theoretic modeling to explore the connections between privacy, polarization, and the divisiveness of laws. Our framework is based on a population of citizens that may be more or less polarized. A law is defined in terms of its effect on each citizen and must gain support from a majority in order to pass. We define a notion of divisiveness which allows us to measure the extent to which a law disproportionately affects different groups of citizens. Our framework allows us to explore four distinct notions of privacy, two that result from technological measures and two that emerge from legal theory. We find that privacy can prevent the passage of certain divisive laws, but the effects depend strongly on which type of privacy is in use.

Keywords: Privacy, Polarization, Law, Search, Marginalized Populations

1 Introduction

In 2006, Utah police received an anonymous tip about drugs being sold out of a house in South Salt Lake. Detective Douglas Fackrell spent several hours surveilling the house in an unmarked car, but saw only modestly suspicious activity. After a week, he stopped an individual, Edward Strieff, as he was exiting the house and asked for identification. When he discovered that Strieff had an outstanding warrant for a minor traffic violation, Detective Fackrell proceeded to search him and found methamphetamine in Strieff's pockets.

This event marked the start of legal battle that reached the US Supreme Court this year. Although a warrant generally provides adequate reason for a search, the police conceded that Fackrell did not have reasonable suspicion to detain Strieff in the first place. The supreme court has long held that evidence gained in violation of the Fourth Amendment is inadmissible as evidence - the so-called exclusionary rule. The case revolves around the extent to which the exclusionary rule protects the privacy of citizens when new information, such as an arrest warrant, arrives after an improper detainment.

Utah v. Strieff reveals the extent to which our value of privacy is bound up in notions of power and polarization. During oral argument in February, Justice Sonya Sotomayor posed the following question.

> “What stops us from becoming a police state and just having the police stand on the corner down here and stop every person, ask them for identification, put it through, and if a warrant comes up, searching them?"

At the heart of this argument is a recognition that privacy protects entire groups of people. One doesn’t have to have drugs in one’s pocket to object to arbitrary searches by police. Privacy places limitations on police power, affecting the playing field faced by all citizens. Even when the vast majority of police officers abide by strict ethical standards, the prospect of running into a corrupt one remains threatening. Furthermore, the ability to invade the privacy of citizens has been argued to increase incentives for governments to abuse their power. [25]

Calls for privacy are particularly acute when a particular group is disadvantaged or marginalized. In this case, the laws that police enforce may disproportionally affect the marginalized group. A classic example is the disparity between sentences for powder cocaine, typically associated with rich white communities, and crack cocaine, which is associated with disadvantaged black communities. Before the fair sentencing act of 2010, the weight of powder cocaine needed to trigger certain federal criminal penalties was 100 times greater than the weight of crack cocaine that would trigger the same penalties. This disparity is said to be a significant factor behind the large number of African Americans that were sentenced for drug offenses. [8]

To understand how laws and police enforcement affect disadvantaged groups, we must also understand how society is polarized between different groups of people to begin with. How are laws passed that benefit one group at the expense of another group. Moreover, can privacy protection help marginalized groups overcome their disadvantageous position?

In this paper, we use game theoretic modeling to explore the connections between privacy, polarization, and the passage of divisive laws. Our framework is based on a population of citizens that influence what laws are passed, or what laws are maintained. A law is defined in terms of how it impacts each individual, and our model is flexible in that it allows any set of effects. We define a notion of divisiveness which allows us to measure the extent to which a law disproportionately affects different groups of citizens.

Divisiveness is not the only factor to consider when evaluating laws. A divisive law may still be justified if it significantly improves welfare. Progressive taxation is one example in which a law targets groups differently with the frequent aim of enhancing welfare. On the other hand, some laws may not be divisive at all, but may still be welfare-decreasing or unjust for other reasons. Nevertheless, we believe that divisiveness should generally be viewed as a cause for concern, especially when a law targets a marginalized group.

Our framework allows citizens to form opinions based on how a law impacts them directly, but it optionally allows them to consider the impact on others as well. This is achieved through an influence matrix that is multiplied by the direct effect of the law. This can be used to represent a concern for friends, loyalty to a larger group, or learning from a small number of influential personalities. The influence matrix also allows us to discuss how polarized society is. At the end of our analysis, we construct a matrix to model the case of a society with one majority group and one minority group.

Our model assumes that laws that are supported by a majority of citizens are passed or maintained. Although the democratic process involves many factors before gathering a simple majority, we believe this is a useful and tractable way to explain the types of laws that exist in society.

Using our model of how laws are enforced, we are able to identity four distinct notions of privacy. Two of these are technological, including strategies that citizens can take to hide features and behaviors from authorities. The other two are legal notions, depending on a judicial branch that functions as a check on enforcement procedures. We describe the function of each of these privacy notions using our two-population model of society. We find that each type of privacy allows a different set of laws to be passed and enforced, resulting in different effects on divisiveness. Our work supports the idea that privacy, while far from a perfect cure, has a role to play in mitigating the divisive effects of laws in a polarized society.

2 Related work

2.1 Privacy and Government

This work falls within a line of research that investigates the balance of power between citizens and the state. In [25], we investigated the application of surveillance technology by a government that wishes to remain in power. Our main takeaway was that enhanced surveillance technology increases incentives for abuse.

In a similar vein, Goh provides a model of a government that may employ surveillance to lower the risk of a terrorist attack [15]. Greater surveillance carries an increased risk that citizens will learn of its existence, which increases the risk that the government loses power. Goh finds that a rational government will employ less surveillance when citizens value their privacy more, but autocratic governments will employ more surveillance than democratic ones.

A larger literature examines the relationship between citizens and the state in general. Downs [13] provides a model of political competition based on a continuum of political preferences, extending Hoteling's study of horizontal differentiation [31]. Further studies model the process by which governments are overthrown. Ginkel and Smith [14] consider factors that determine the probability of revolution in a repressive regime. Lohmann [27] describes the potential overthrow of a government through an informational cascade model. Kuran [21] attempts to explain why revolutions often take the world by surprise with a game theoretic model of political change. These studies do not consider the effects of privacy in determining political outcomes.

2.2 Privacy and Firms

Privacy also affects the relationship between citizens and firms, and several strands of research shed light on this topic (Acquisti provides a survey [1]). Privacy can be seen in the classic literature on information economics as an information imbalance between a principal and an agent. Moral hazard models assume that an agent's actions are not directly observable and the focus is on aligning incentives through contracting [19] [35]. In models of adverse selection, agent types are private and certain types are driven out of a market because the principal cannot distinguish between them [4]. In signaling games, agents may engage in costly actions to signal their private type for economic gain [34]. None of these settings correspond to our focus on privacy as protecting a marginalized group. Furthermore, models in this literature are usually neoclassical in the sense that privacy is an obstacle to maximizing welfare.

An emerging body of privacy research models the behavior of consumers that participate in two different markets in sequence. Firms in one market learn about consumers based on their purchase decisions and may be allowed to sell this information to firms in the second market. A common theme in this literature is the fact that outcomes depend on whether consumers are myopic, considering each purchase decision without regard for how it will affect future purchases, or fully sophisticated. In [20], we found that when consumers are myopic, firms benefit greatly, but consumer surplus is also reduced. When we assume that consumers are strategic, consumers are better off, but firms fare worse. In a similar vein, Acquisti and Varian look at a single monopolist that sells two goods in series [3]. Taylor examines the case of two firms when consumer valuations for each good can take on two values, but these valuations are not perfectly correlated with each other [38]. Information sharing may increase or decrease consumer surplus and welfare, depending on the demand specification.

Other studies provide further examples of scenarios in which privacy is welfare-enhancing. Hermalin and Katz discuss insurance markets and investments in information gathering [17]. Taylor considers a scenario in which collecting information about customers is costly and firms may overinvest in this activity [37]. Hann et al. argue that unsolicited marketing imposes negative costs on consumers in the absence of privacy regulation [16].

A final literature studies privacy through the lens of mechanism design. Calzolari and Pavan describe a framework in which firms may offer arbitrary contracts to users [10]. A set of recent papers have pioneered the use of differential privacy as a solution concept [29]. In these models, agents must be approximately truthful to the mechanism and cannot change the outcome by very much if they lie or refuse to participate. Protecting privacy is not the focus of these models, since the solution concept begins with an assumption that agents don't hide information.

In contrast to the studies we mention, which treat privacy as a binary parameter, our work distinguishes four distinct types of privacy, which are inspired by technologies and legal debate. We further apply our model to explore the effects of privacy on divisive laws.

2.3 Technological Features of Privacy

Citizens that engage in behavior that is forbidden by a law may employ privacy-enhancing technologies, such as the anonymizing Tor network [12]. Sweeney defines a notion, k-anonymity, to measure the anonymity provided by a particular dataset [36]. Technologies also mediate the enforcement of laws. The ability of a government to identify law-breakers is enhanced through techniques like dataset aggregation [2]. An ongoing debate surrounds the use of these and other technologies, in contexts ranging from ethics [11, 28], to law [5, 22–24], to security-relevant effectiveness [32]. While our model abstracts from these details, we will use it to explore the impact of technologically-based privacy.

2.4 Polarization

Most voters in the United States are overwhelmingly moderate in their policy positions [26]. Nevertheless, the United States Congress has passed a number of divisive laws, many of which have been challenged and overturned by the US Supreme Court. Divisive laws have also been passed in European countries, including those against face covering, pejoratively dubbed "burka bans."

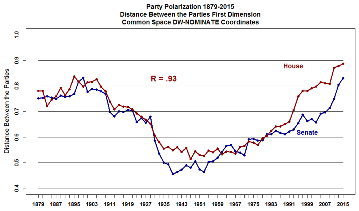

Fig. 1. Polarization Trends in the US Congress

The United States congress in particular has become increasingly polarized over the last 40 years (see Figure 1). Today, members of congress exhibit a distinctly bimodal distribution in terms of political preferences, as seen in 2. Researchers have posited a number of reasons for this phenomenon [6] [30], ranging from a polarized electorate, to southern realignment, to gerrymandering, to the evolution of modern primary elections, to economic inequality, to money in politics, to the media environment, or to congress-based factors such as congressional rule changes, majority party agenda control, party pressures, teamsmanship, or the breakdown of bipartisan norms. All of these issues are discussed in [30]. More culturally-specific theories involving authoritarianism are also prevalent [18].

A more economically-driven explanation derives from the notion of information cascades. An information cascade occurs when people receive a noisy informational

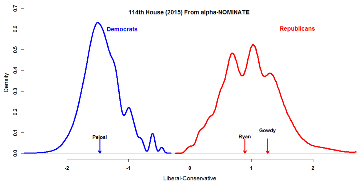

Fig. 2. Partisonship in the US House of Representatives

signal and observe the behavior of friends and colleagues to inform decision-making. Although agents are individually rational, they may find it optimal to rely on the information they derive from previous agents, ignoring their private signals [9].

The notion that people exhibit herding behavior in predictable circumstances has been around for decades [33]. For example, researchers at Iowa State University conducted 259 interviews with farmers who had largely refused offers to adopt drought-resistant seed corn during the Great Depression and Dust Bowl. They found that the slow rate of adoption was due to "how farmers valued the opinion of their friends and neighbors instead of the word of a salesman" [7].

We include a notion of influenced behavior in our model as a way to describe the polarization of society. Our model does not mandate that citizens consider how a law affects other citizens, but merely allows it.

3 Model

3.1 Definitions

As we use the terms divisiveness, polarization, and privacy throughout the paper, we take care to define them here.

- *Divisiveness* of a law refers to the extent to which the different citizens value the law differently – measured, for example, by the standard deviation in valuations.
- *Polarization* of a society with respect to a law refers to the grouping of individuals into sets having disparate valuation of that law.
- *Privacy* refers to an individual's ability to possess property (physical or intellectual) that is free from inspection or search.

3.2 Overview

Our general model presents an incentive structure for explaining polarization of a society with respect to divisive laws. Given a specific law, our model assumes the following.

- Each individual begins with an initial evaluation of the law. We refer to this initial evaluation as the derived benefit for that individual.
- Each individual's support for a law may (but need not) be influenced by other individuals.
- Individuals are heterogeneous in their ability to influence others.

3.3 Citizen Influence

For each pair of citizens

$$i, j \in \{1, \ldots N\},$$

define

$$a_{ij} \in [0, 1]$$

to be the influence of person j on person i. We may think of a_{ij} also as the affinity person i has toward person j.

Each individual will arrive at a level of support for the law based on a weighted average of the valuations of their influences, where the weighting is determined by the influence parameters a_{ij}. To be consistent with the notion of weighted average, we thus require

$$\sum_j a_{ij} = 1.$$

3.4 Citizen Valuations of Laws

Given a law L and a citizen $j \in \{1, \ldots N\}$, let

$$V_L(i) \in \mathbb{R}$$

represent the direct impact of the law on person i. We assume that the direct impact of L is unbounded because laws may save a life or take away life from individuals impacted by them.

If an individual's direct valuation for a law is perfectly in tune with the direct impact on the law then this person's support for a law will be $V_L(i)$. In other cases, for example where a law has little or no direct impact on the individual, a ban on muslims for example, initial evaluation of the law may be something very close to zero, i.e. neither positive nor negative. Nevertheless a person's view of the law may evolve based on the views and experiences of their influences. In such cases, we may suppose that after some amount of time, an individual's support for L evolves to become

$$U_L(i) = \sum_j a_{ij} V_L(j).$$

4 Analysis

4.1 A Law Valuation Functional Form

In this section, we specify a functional form for V_L in order to discuss the effects of privacy. While this reduces the generality of our model, it allows us to distinguish between different notions of privacy protection.

We imagine that three conditions must apply for citizen i to be punished by a law:

1. As the text of the law is written, it specifies that citizen i is engaged in unlawful behavior. We assume this occurs with probability $C(i)$.
2. Citizen i is searched by the authorities. We assume this occurs with probability $S(i)$.
3. A search on citizen i is successful in finding evidence. Conditional on the previous conditions, we assume this occurs with probability $F(i)$. For simplicity, we will assume this function is a constant and write it as F.

The probability that citizen i is punished is therefore $S(i)C(i)F$. Let P be the punishment for violating the law. Then each citizen's individual utility based only on the law's expected punishment on them may be given by

$$S(i)C(i)F \cdot P.$$

We may also compute the total number of citizens punished by the law as

$$\sum_j S(j)C(j)F.$$

As far as the benefits of a law go, we assume that each individual i suffers a cost l_i each time a particular crime is committed. This may be interpreted to include direct effects (e.g. the individual is targeted by theft or violence) as well as indirect effects (e.g. the prevalence of a crime makes the individual feel less welcome in their community). For the current analysis, we assume that the number of crimes is reduced by exactly the number of people punished. In other words, we do not allow for deterrent effects. If such effects exist, they may multiply the effects of each search, and they may cause non-linearities in the valuation functions. We defer these interesting issues to a future analysis.

Given these assumptions, we can write the initial valuation of law L to person i as the difference between the benefit gained from less crime and the individual's expected punishment in case she breaks the law. That is,

$$V_L(i) = l_i \sum_j S(j)C(j)F - S(i)C(i)F \cdot P$$

4.2 Four Types of Privacy

Our valuation model allows us to compare four types of privacy, the first two of which are technological in nature, and the second two of which are legal.

Attribute Privacy Attribute privacy is the notion that a person can conceal personal characteristics, which authorities may use to identify them as someone likely to commit a crime. *Attribute privacy serves to prevent targeted searches.* An example in which the attributes of individuals are fully or nearly anonymized is the case in which users of TOR hide their online activities. We may model this type of privacy by stipulating that $S(i)$ is a constant.

$$S(i) = S$$

For a given text of a law, which implicitly specifies for each citizen i the probability with which they are a criminal with respect to the law, restrictions on $S(i)$ (the probability that a citizen is searched) may prevent a majority from emerging to support the law. In practice, when individual-targeted searches are prevented, we may expect authorities to restrict searches to a minority of the population, thereby ensuring that $V_L(i)$ is positive for a majority of individuals.

In this case, the shape of V_L is entirely determined by the distribution of criminal behavior. Thus the number of individuals that support the law depends only on $C(i)$ and how polarized society is.

Search Privacy Search Privacy is the idea that a citizen may use technology to prevent the discovery of evidence in the event that she is searched. We represent this as a decrease in the parameter, F,

$$F < 1$$

representing the chance that evidence is found when a citizen breaking the law is searched. In our valuation model, F appears in both the positive and negative components of V_L so that it does not change the number of citizens supporting the law.

Nevertheless, this type of privacy will affect welfare, scaling it towards zero. Search privacy may therefore be welfare-benefitting in the case of divisive laws for which welfare is negative.

Search Quantity Privacy Our first legal notion of privacy corresponds to the idea that searches should not be widespread in a society. Commentary discussed in the introduction involving the recent supreme court case Utah v. Strieff exemplifies this notion. We encode this notion of privacy in our valuation model by requiring that the fraction of citizens that are searched is less than some bound,

$$\frac{\sum_j S(j)}{n} < m \tag{1}$$

Laws that don't meet this requirement may be declared unenforceable. Search Quantity Privacy prevents the enforcement of laws against a large fraction of a population.

Search Specificity Privacy Another notion of privacy supposes that authorities must have individualized reasonable suspicion to conduct a search. This is similar to the notion of Search Quantity Privacy, defined above, but the focus is not on the total proportion of searches with respect to a population, but rather on how well-targeted the searches are. We may encode this notion of privacy by requiring that a certain fraction of searches result in the finding of evidence,

$$\frac{\sum_j S(j)C(j)F}{\sum_j S(j)} > \rho \tag{2}$$

4.3 A Two-Party Influence Framework

To further explore issues of privacy, we will place additional structure on citizen affinity. In this section, we analyze the special case that there are two subsets of citizens, labeled G_0 and G_1. Citizens in G_0 are assumed to form the majority with population n_0. Citizens in G_1 form the minority with population $n_1 < n_0$. We will also refer to members of G_0 and G_1 as type 0 and type 1, respectively. We assume that all members of a group G_k share the same probability of breaking a law, labeled $C(k)$, the same probability of being searched, labeled $S(k)$. We also assume all citizens share the same direct cost for each crime committed, labeled l.

Within each group, we further assume that all citizens share the same level of support for all laws. For example, one way for this to happen would be if the influence function a_{ij} itself were constant within each of the four cases $i, j \in G_0$; $i \in G_0, j \in G_1$; $i \in G_1, j \in G_0$; and $i, j \in G_1$. In this case, regardless of any individual's initial valuation of a law, the resulting final support for the law would be uniform within each group.

As another example, we could assume that each of the two subgroups of citizens included a single influential thought leader, labeled $t_0 \in G_0$ and $t_1 \in G_1$. Suppose that every individual only had positive affinity for these two thought leaders, and the vector of affinities within each group was uniform. In terms of final support for a law, this scenario is indistinguishable from the example above.

Regardless of how support is formed, we will use the notation $A_{00} = \sum_{i,j \in G_0} a_{ij}/n_0^2$ to represent the average affinity an individual in the majority has for other majority individuals. We use $A_{01} = \sum_{i \in G_0, j \in G_1} a_{ij}/n_0 n_1$ to represent the average affinity a member of the majority has for members of the minority, and so forth for the other cases.

Our last assumption encodes some degree of polarization in this society. We assume that each group has a higher inter-group affinity than a cross-group affinity. That is,

$$A_{00} > \frac{1}{N} = \frac{1}{n_0 + n_1} > A_{01} \tag{3}$$

$$A_{11} > \frac{1}{N} = \frac{1}{n_0 + n_1} > A_{10} \tag{4}$$

Given a law (C, S, F), let $p_0 = C(0)S(0)F$ be the fraction of the majority that are punished, and let $p_1 = C(1)S(1)F$ be the fraction of the minority that are punished. We use Figure 3 to plot these quantities for different possible laws. On this graph, the x-axis represents p_0 and the y-axis represents p_1. In our model, the text of the law specifies the maximum fraction of each type of citizen that can be punished, $C(0)$ and $C(1)$, which occurs when $F = 1$ and everyone is searched. This region is represented by the outermost rectangle in the Figure, labeled A.

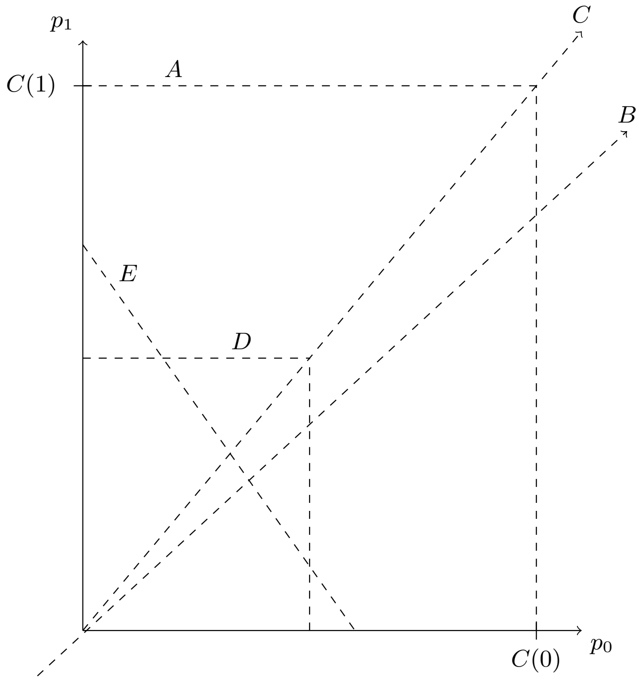

Fig. 3. This figure shows the effects of privacy on divisive laws.

Since more than half of the population is in G_0, a law may pass whenever the support of each type 0 individual is nonnegative. We may compute support from individuals of type 0 as follows,

$$
\begin{aligned}
U_L(i)(0) &= n_0 A_{00} V_L(0) + n_1 A_{01} V_L(1) && (5)\\
&= n_0 A_{00}[l(p_0 n_0 + p_1 n_1) - p_0 P] + n_1 A_{01}[l(p_0 n_0 + p_1 n_1) - p_1 P] && (6)\\
&= l(p_0 n_0 + p_1 n_1) - n_0 A_{00} p_0 P - n_1 A_{01} p_1 P && (7)\\
&= [l - PA_{00}] n_0 p_0 + [l - PA_{01}] n_1 p_1 && (8)\\
& && (9)
\end{aligned}
$$

Letting $b_{00} = l - PA_{00}$ and $b_{01} = l - PA_{01}$, we can write,

$$U_L(0) = b_{00}n_0p_0 + b_{01}n_1p_1 \tag{10}$$

Our assumption that $A_{00} > A_{01}$ guarantees that $b_{00} < b_{01}$. This means that there are 3 possibilities for the signs of the coefficients on p_0 and p_1.

1. $\partial U_L(0)/\partial p_0 \leq 0$ and $\partial U_L(0)/\partial p_1 \leq 0$. This will happen whenever $l \leq A_{01}P$, meaning that the benefit from the law is small relative to the size of the punishment multiplied by the affinity of the majority for the minority.
2. $\partial U_L(0)/\partial p_0 \leq 0$ and $\partial U_L(0)/\partial p_1 > 0$. This will happen whenever $A_{01}P < l \leq A_{00}P$, or for intermediary amounts of benefit. In this case, the majority will tend to support laws that punish the minority more and the majority less.
3. $\partial U_L(0)/\partial p_0 > 0$ and $\partial U_L(0)/\partial p_1 > 0$. This will happen whenever $A_{00}P < l$, or for high amounts of benefit. In this case, the majority will tend to support laws that punish both groups as much as possible.

The middle possibility, in which majority support increases with p_1 but decreases with p_0 is of particular interest, since this is the case in which the majority would favor the most divisive treatment of the two groups.

A law will have majority support if and only if $U_L(0) \geq 0$. This can be written as,

$$U_L(0) = b_{00}n_0p_0 + b_{01}n_1p_1 \geq 0 \tag{11}$$

If condition 1 holds above, no law within rectangle A can have majority support, except for the origin. This means that nobody will be punished and no benefit results. If condition 3 holds above, every law within rectangle A has majority support, so a law may pass for any values of $S(0)$, $S(1)$, and F. For the more interesting condition 2, the previous equation divides rectangle A into two regions. This is depicted by line B in Figure 3. Every law that falls on this line or above can have majority support.

Using a similar argument to that above, we can derive the support of a type 1 citizen for the law to be

$$U_L(1) = b_{10}n_0p_0 + b_{11}n_1p_1 \tag{12}$$

where $b_{10} = l - A_{10}P$ and $b_{11} = l - A_{11}P$. Since we assume $A_{10} < A_{11}$, we have $b_{10} > b_{11}$.

We compute divisiveness as the standard deviation,

$$s_L = \sqrt{var(U_L)} = \sqrt{E\left[\left(U_L - \bar{U_L}\right)^2\right]} \tag{13}$$

$$= \sqrt{\frac{n_0\left(U_L(0) - \bar{U_L}\right)^2 + n_1\left(U_L(1) - \bar{U_L}\right)^2}{n_0 + n_1}} \tag{14}$$

where $\bar{U_L} = \frac{n_0 U_L(0)+n_1 U_L(1)}{n_0+n_1}$ is the average support for the law. After some algebra, this can be simplified to the following,

$$s_L = \frac{\sqrt{n_0 n_1}}{n_0 + n_1} \left| U_L(0) - U_L(1) \right| \tag{15}$$

In the region of laws that have majority support, it can be shows that $U_L(0) > U_L(1)$. Substituting for $U_L(0)$ and $U_L(1)$, we have

$$\begin{aligned} s_L &= \frac{\sqrt{n_0 n_1}}{n_0 + n_1} \left(b_{00} n_0 p_0 + b_{01} n_1 p_1 - b_{10} n_0 p_0 - b_{11} n_1 p_1 \right) && (16) \\ &= \frac{\sqrt{n_0 n_1}}{n_0 + n_1} \left((b_{00} - b_{10}) n_0 p_0 + (b_{01} - b_{11}) n_1 p_1 \right) && (17) \\ &= \frac{\sqrt{n_0 n_1}}{n_0 + n_1} \left((A_{10} - A_{00}) P n_0 p_0 + (A_{11} - A_{01}) P n_1 p_1 \right) && (18) \\ & && (19) \end{aligned}$$

by the ordering on our affinities, we know $A_{10} - A_{00} < 0$ and $A_{11} - A_{01} > 0$ so

$$\begin{aligned} \partial s_L / \partial p_0 &< 0 && (20) \\ \partial s_L / \partial p_1 &> 0 && (21) \end{aligned}$$

In other words, in the region of laws with majority support, divisiveness goes up with the number of minority members punished and down with the number of minority members punished. This means that the law most favored by the majority, which is in the upper left corner of rectangle A, is also the most divisive.

4.4 Privacy Effects

Having outlined some basic properties of our model, we turn our attention to the effects of different types of privacy.

Effects of Attribute Privacy We begin with attribute privacy, which we understand to mean restrictions on S(0). We model the extreme case of anonymity, represented as $S(0) = S(1)$. The set of possible laws is represented by line C in Figure 3. Note that line C passes through the point $(C(0), C(1))$ at the upper right of rectangle A. A more moderate version of attribute privacy may place bounds on the ratio of $S(1)$ to $S(0)$. For example, we may specify,

$$0 < \underline{\mathrm{r}} < S(1)/S(0) < \bar{r} < \infty \tag{22}$$

Since divisiveness is maximized at the point $(0, C(1))$, attribute privacy necessarily reduces the maximum amount of divisiveness since it disallows laws at this point. As the figure is depicted, the slope of line C is greater than the slope of line B,

$$C(1)/C(0) > -b_{00}n_0/b_{01}n_1 \tag{23}$$

This means that any law that falls inside line C and rectangle A will also have majority support. The majority would offer the most support to laws that fall further to the upper right of the line. It is also possible, for the slope of line C to be less than the slope of line B,

$$C(1)/C(0) > -b_{00}n_0/b_{01}n_1 \tag{24}$$

In this case, no law on line C will have majority support except for a law at the origin. Nevertheless, divisiveness decreases since having no law or a law at the origin brings divisiveness to zero.

Effects of Search Privacy We interpret search privacy to mean that not all individuals who are searched while committing a crime are caught,

$$F < 1 \tag{25}$$

This condition limits the maximum number of people, of either type, who may be punished. This is depicted by rectangle D in Figure 3. Like attribute privacy, search privacy reduces the maximum amount of divisiveness that can be caused by a law. Specifically, the maximum divisiveness is reduced by a factor of F. Unlike attribute privacy, search privacy never results in a scenario in which a previously enforced law can no longer have majority support. As long as $S(0)$ and $S(1)$ are unchanged, reducing F still results in a law with majority support. Divisiveness and welfare are simply scaled downwards.

Effects of Search Quantity Privacy To model a policy of search quantity privacy, we impose the condition,

$$\frac{n_0S(0) + n_1S(1)}{n_0 + n_1} < m \tag{26}$$

The maximum value of $S(0)$ can be attained when $S(1) = 0$, allowing $S(0) = m(n_0 + n_1)/n_0$. Similarly, when $S(0) = 0$, $S(1)$ can attain a value of $S(1) = m(n_0 + n_1)/n_1$. Note that the maximum value of $S(0)$ is smaller than the maximum value of $S(1)$. This feature is plotted as line E in Figure 3. Laws below this line are acceptable under the search quantity standard.

As the figure demonstrates, search quantity privacy may reduce the maximum possible divisiveness of a law. The majority will still favor a law that is at the top corner of the acceptable region, which represents the maximum amount of divisiveness for a given amount of searches. If the bound m is not set low enough, the maximum amount of divisiveness may not be reduced at all.

Effects of Search Specificity Privacy Search Specificity Privacy requires a certain proportion of searches to turn up evidence that an individual is breaking the law. We represent this by writing,

$$\frac{\sum_j S(j)C(j)F}{\sum_j S(j)} = \frac{n_0 S(0)C(0)F + n_1 S(1)C(1)F}{n_0 S(0) + n_1 S(1)} > \rho$$

Rearranging,

$$\begin{aligned} n_0 S(0)C(0)F + n_1 S(1)C(1)F &> \rho n_0 S(0) + \rho n_1 S(1) \\ (n_1 C(1)F - \rho n_1)S(1) &> -(n_0 C(0)F - \rho n_0)S(0) \end{aligned} \tag{27}$$

When ρ is close enough to 0, the left hand side is nonnegative and the right hand side is nonpositive, so the constraint does not bind. The set of possible laws is therefore not reduced. On the other hand, when ρ is close enough to 1, the left hand side is nonpositive and the right hand side is nonnegative, so the constraint binds unless $S(0) = S(1) = 0$. No law can pass the privacy requirement except for the trivial one that doesn't punish anyone.

The more interesting region is when ρ lies between $C(0)F$ and $C(1)F$. In the case that $C(1) > C(0)$, meaning that the text of the law targets behavior that is more common for individuals of type 1, we can write the constraint as,

$$\frac{S(1)}{S(0)} > \frac{\rho n_0 - n_0 C(0)F}{n_1 C(1)F - \rho n_1} \tag{28}$$

where the fraction is arranged so that the numerator and denominator are positive. This constraint is depicted by line F in Figure 3. Every law above this line is permitted under the search specificity rule. Unfortunately, this rule does nothing to reduce the maximum possible divisiveness of a law. In fact, it may have the opposite effect, allowing only laws for which members of the minority are much more likely to be searched than members of the majority.

In part, this conclusion may be the result of limitations of our model. We have assumed that all members within a group have equal odds of breaking the law and equal odds of being searched. A more detailed model might allow individuals to vary within each group. Authorities may be able to select a smaller fraction of each group, choosing individuals with a higher probability of breaking the law, thereby increasing the proportion of searches that turn up evidence. In such a model, search specificity privacy may be expected to limit the maximum divisiveness of a law. Nevertheless, we believe that our central insight, that search specificity privacy limits searches on the majority more than on the minority, will continue to hold.

5 Discussion and Conclusion

Our study is an attempt to understand privacy, not at the level of individual incentives, but at the level of communities and the relationships they have to each other and to the state. Though our modeling framework is exploratory, it reveals some of the complexity inherent in these relationships. We were able to relate privacy to polarization and the divisiveness of laws, but found that outcomes depend critically on what notion of privacy is in play. Privacy enforced through technology can have dramatic effects on what laws are enforced, but all laws may be rendered ineffective whether divisive or not. A privacy technology may work, after all, whether it is concealing sexual behavior between consenting adults, or a plot to assassinate a leader in government. Legal notions of privacy hold the promise of more precise judgements. Courts can identify disadvantaged groups and extend protections to them, without extending those same protections to say, serial killers. Yet our model predicts that here too, privacy is not perfectly tailored to prevent the enforcement of divisive laws. Further research is needed to assess how privacy laws may work in conjunction with anti-discrimination laws and policies, to better protect marginalized groups.

In the future, we plan to extend our model to capture more features of the legal system and of privacy protection. One important addition will be a description of how authorities gather information on potential law breakers. A detailed model might describe citizens with a collection of attributes, each of which may carry information about a citizen's propensity to violate a specific law. Some attributes may be hidden with technological privacy measures, some may be the topic of legal protection, and others may remain public and available to police as they direct their investigations.

We would further like to model the issues that arise when police have the right to search a large number of people, but only enough resources to choose a small number. The ability to arbitrarily select which citizens to search carries a significant amount of power, even when the number of searches remains small. A more complete model would separate legality from the actual performance of a search in order to highlight these issues.

As technology advances, many established notions of privacy face considerable pressure to evolve. Location monitoring, deep packet inspection, linking of consumer databases, and face recognition are just a few of the threats to our ability to control our personal information. We hope that studies like ours will help spur discussion about the role privacy plays in maintaining balances of power, and how future definitions of privacy may best be structured to protect vulnerable groups and individuals.

Acknowledgments ...

References

1. Acquisti, A.: The economics of personal data and the economics of privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable 1 (2010)
2. Acquisti, A., Gross, R.: Predicting social security numbers from public data. Proceedings of the National academy of sciences 106(27), 10975–10980 (2009)
3. Acquisti, A., Varian, H.R.: Conditioning prices on purchase history. Marketing Science 24(3), 367–381 (2005)
4. Akerlof, G.: The market for ?lemons?: Quality uncertainty and the market mechanism. Springer (1995)
5. Bankston, K., Soltani, A.: Tiny constables and the cost of surveillance: Making cents out of united states v. jones. Yale Law Journal Online 123 (2014)
6. Barber, M., McCarty, N.: Causes and consequences of polarization. Solutions to Political Polarization in America 15 (2015)
7. Beal, G.M., Bohlen, J.M., et al.: The diffusion process. Agricultural Experiment Station, Iowa State College (1957)
8. Beaver, A.L.: Getting a fix on cocaine sentencing policy: reforming the sentencing scheme of the anti-drug abuse act of 1986. Fordham L. Rev. 78, 2531 (2009)
9. Bikhchandani, S., Hirshleifer, D., Welch, I.: A theory of fads, fashion, custom, and cultural change as informational cascades. Journal of political Economy pp. 992–1026 (1992)
10. Calzolari, G., Pavan, A.: On the optimality of privacy in sequential contracting. Journal of Economic Theory 130(1), 168–204 (2006)
11. Diffie, W., Landau, S.: Privacy on the Line: The Politics of Wiretapping and Encryption. The MIT Press, updated and expanded edition edn. (Feb 2010), http://www.worldcat.org/isbn/0262514001
12. Dingledine, R., Syverson, P.F.: Privacy enhancing technologies. Springer (2003)
13. Downs, A.: An economic theory of political action in a democracy. The journal of political economy pp. 135–150 (1957)
14. Ginkel, J., Smith, A.: So you say you want a revolution a game theoretic explanation of revolution in repressive regimes. Journal of Conflict Resolution 43(3), 291–316 (1999)
15. Goh, B.: Prosperity and security: A political economy model of internet surveillance (2015)
16. Hann, I.H., Hui, K.L., Lee, S.Y.T., Png, I.P.: Consumer privacy and marketing avoidance: A static model. Management Science 54(6), 1094–1103 (2008)
17. Hermalin, B.E., Katz, M.L.: Privacy, property rights and efficiency: The economics of privacy as secrecy. Quantitative Marketing and Economics 4(3), 209–239 (2006)
18. Hetherington, M.J., Weiler, J.D.: Authoritarianism and polarization in American politics. Cambridge University Press (2009)
19. Hölmstrom, B.: Moral hazard and observability. The Bell journal of economics pp. 74–91 (1979)
20. Johnson, B., Laskowski, P., Maillart, T., Chuang, J., Christin, N.: Caviar and yachts: How your purchase data may come back to haunt you
21. Kuran, T.: Sparks and prairie fires: A theory of unanticipated political revolution. Public choice 61(1), 41–74 (1989)
22. Landau, S.: National Security on the Line. Social Science Research Network Working Paper Series (Apr 2009), http://ssrn.com/abstract=1166155

23. Landau, S.: Making sense from snowden: What's significant in the nsa surveillance revelations. IEEE Security and Privacy 11(4), 54–63 (2013)
24. Landau, S.: Making sense of snowden, part ii : What's significant in the nsa revelations. IEEE Security and Privacy 12(1), 62–64 (2014)
25. Laskowski, P., Johnson, B., Maillart, T., Chuang, J.: Government surveillance and incentives to abuse power
26. Layman, G.C., Carsey, T.M., Horowitz, J.M.: Party polarization in american politics: Characteristics, causes, and consequences. Annu. Rev. Polit. Sci. 9, 83–110 (2006)
27. Lohmann, S.: The dynamics of informational cascades: The monday demonstrations in leipzig, east germany, 1989–91. World politics 47(01), 42–101 (1994)
28. Lyon, D.: Surveillance as social sorting: privacy, risk, and digital discrimination. Psychology Press (2002)
29. Pai, M.M., Roth, A.: Privacy and mechanism design. ACM SIGecom Exchanges 12(1), 8–29 (2013)
30. Poole, K.T., Rosenthal, H.: The polarization of american politics. The Journal of Politics 46(04), 1061–1079 (1984)
31. Press, O.: Hotelling (1929),? stability in competition? Economic Journal 39
32. Schneier, B.: It for oppression. Security & Privacy, IEEE 11(2), 96–96 (2013)
33. Shiller, R.J.: Conversation, information, and herd behavior. The American Economic Review 85(2), 181–185 (1995)
34. Spence, M.: Job market signaling. The quarterly journal of Economics pp. 355–374 (1973)
35. Stiglitz, J.E., Weiss, A.: Credit rationing in markets with imperfect information. The American economic review 71(3), 393–410 (1981)
36. Sweeney, L.: k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10(05), 557–570 (2002)
37. Taylor, C.R.: Privacy in competitive markets. Tech. rep. (2003)
38. Taylor, C.R.: Consumer privacy and the market for customer information. RAND Journal of Economics pp. 631–650 (2004)