

Reforming the Privacy/Security Debate: The Problem with Justification Standards

DRAFT VERSION: PLEASE DO NOT CITE

Paul Ohm*

Before the police can access sensitive, private data, they must often meet statutory justification standards, proving to a judge that they have probable cause, reasonable suspicion, or can assert the relevance linking the information to a crime or suspect. Scholars and policymakers have borrowed these justification standards from Constitutional Criminal Procedure, believing that these standards somehow discipline police behavior. For the most part, they are wrong.

Justification standards don't require the police or judges to balance privacy and security. Instead, these standards focus solely on what the police can prove, in other words on police need. Furthermore, there is reason to believe that the differences between the various standards aren't that meaningful, especially in a typical, data-intensive, twenty-first century criminal investigation. Worse, the reliance on these standards as the sole means for regulating the line between privacy and security has led directly to the winner-take-all, zero-sum nature of the privacy debate.

This article argues for new statutes that force the police and judges to weigh privacy and security in every situation. Laws should focus more on what the police have done and the choices they have made than on merely what they think they can prove. In the end, these laws will also shape the debates about privacy, security, terrorism, and technology, by providing access to legal tools that balance all of these concerns.

*Associate Professor of Law and Telecommunications, University of Colorado Law School.

Table of Contents

INTRODUCTION	3
I. THE DEBATE OVER PRIVACY AND SECURITY: AN IMPOSSIBLE BALANCE	5
A. TWO SCHOLARLY SHIPS, PASSING IN THE NIGHT	5
B. AN INTRACTABLE COLLISION OF INTERESTS.....	9
C. A RHETORICAL DRAG RACE.....	10
II. POOR TOOLS FOR BALANCING	12
A. THE WRONG TOOLS FOR BALANCING	12
B. THE PROBLEM WITH LAW ENFORCEMENT EXCEPTIONS	13
C. THE PROBLEM WITH JUSTIFICATION STANDARDS.....	14
III. WHAT LIES BETWEEN PRIVACY AND SECURITY: INVESTIGATIVE FRICTION	22
A. FRICTION	22
B. FRICTIONAL LAW ENFORCEMENT EXCEPTIONS	23
1. <i>Prioritization</i>	24
2. <i>Tailoring</i>	25
3. <i>Oversight</i>	26
4. <i>Accountability</i>	27
IV. HOW MUCH FRICTION? “GOOD ENOUGH” PRIVACY.....	28
A. HOW MUCH FRICTION?	28
B. HOW MUCH LEGAL FRICTION?	28
1. <i>Tiered Necessity</i>	29
2. <i>A Better Remedy</i>	32
3. <i>A Return to Old-Style Minimization</i>	33
CONCLUSION	33

DRAFT VERSION: PLEASE DO NOT CITE

Introduction

The debate between privacy and security is often described as an epic struggle between important competing interests; in some sense it is the defining struggle of our times. Too often, however, it is treated like parallel morality plays being staged in different cross-town theaters.

On one side of this “debate,” privacy-maximizers spend a lot of time and energy pointing at the immeasurable benefits of privacy, and their only concessions to security are acknowledgments that sometimes privacy’s benefits will be outweighed. On the other side are those—an eclectic group of people with different ideologies who defy easy classification—who claim to balance police interests with privacy interests, but whose methods and conclusions tend to place far too much emphasis on security.

The problem is that the debate has been framed as a winner-take-all, zero-sum game. The metaphor of the balance scale, where one side can weigh a lot more than, a little more than, or the same as the other side does not describe this debate. A better metaphor is a drag race between drivers in two cars on separate lanes of asphalt, each doing little more than pressing harder on the gas. Someone wins; someone loses.

I argue that our adversarial, winner-take-all debate flows directly from the unimaginative solutions we have developed to resolve the debate. Scholars propose and legislators enact laws that supposedly protect privacy, but these laws always include winner-take-all “law enforcement exceptions.” Either the police get to pierce the law’s promise of privacy or they don’t; the police are governed by a trapdoor, a binary condition. They “win” or they “lose” at any given time, and those are the only possibilities. More often than not, they “win,” and these exceptions swallow the rule.

Winner-take-all exceptions lead directly to a winner-take-all debate. With these statutes, there is no room for compromise; there is no space in the middle; there is no sense of balance. We need better solutions, which lead directly to balance. We need solutions that force the police to think hard about the costs of privacy on security before they act and that empower judges to do the same when they review police action.

DRAFT VERSION: PLEASE DO NOT CITE

In this article, I try to identify what those solutions might look like. I try to find the space between privacy and security. In particular, I argue that our law enforcement exceptions need to focus less on what the police can prove and more on what the police have done and the choices they have made. Shining the light on police actions and choices will lead in any particular situation to a debate on the relative importance of privacy and security.

In Part I, I critique the winner-take-all debate, focusing on the arguments that have been made by two groups of scholars. In Part II, I trace the source of this flawed debate to the law enforcement exceptions that have been the only solutions proposed so far for balancing security and privacy. In particular, I question the over-reliance on so-called “justification standards” that measure whether the police have probable cause, reasonable suspicion, or something less tying the evidence sought to the crime or target. I argue that justification standards are much less meaningful, at least when it comes to computerized data and information privacy, than is assumed, and I tie this misunderstanding to a flawed reading of the stop-and-frisk case, *Terry v. Ohio*.

In Part III, I provide an alternative model, which I call investigative friction. There are much better ways to structure law enforcement exceptions to force the police constantly to weigh privacy and security. In particular, I point to four categories of procedures that do a better job than simple justification standards at forcing a balancing approach.

Finally, in Part IV, I argue that investigative friction is best when it makes it *hard but possible* for the police to access especially private or sensitive data. To this end, I propose a few novel solutions—“tiered necessity,” downward sentencing departures in place of suppression, and a return to ex ante minimization—in addition to justification standards.

Of course, even hard but possible covers a spectrum of difficulty and possibilities, and in the end, I don’t pick one spot along that spectrum as optimal. Instead, I suggest that this is the start of an ongoing project and the beginning of a new debate, and policy makers and scholars should ask where they reside along this spectrum, rather than aim for the extremes.

DRAFT VERSION: PLEASE DO NOT CITE

I. The Debate over Privacy and Security: An Impossible Balance

A. Two Scholarly Ships, Passing in the Night

Information privacy¹ is a burgeoning field in which talented scholars have produced dozens of compelling works in the past few years. There are two identifiable strands to this literature, but the authors in each half have not done enough to engage the other side.

On one side is an honest-to-goodness movement, whose authors have been recently twice-branded as members of the “New Privacy” movement² and the “Information Privacy Law Project.”³ Although there are distinctions among the writers in the field, they start from the classical liberal tradition, conceiving information privacy as a fundamental right. What distinguishes the movement, however, are the moves they have made to assign ever more compelling, more universal, and more valuable rights to information privacy, focusing not only on traditional conceptions of individual harm, but recasting the interest as societal. According to them, privacy secures individual autonomy, dignity, and protects a robust, deliberative

¹ The words and definitions used in this field are slippery, and scholars sometimes err by treating alike different concepts relating to information privacy. To try to avoid this pitfall, I will define what I am talking about. This article is about information privacy, defined by many as the right to control personal information. Alan Westin’s definition of privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Many other scholars, government agencies, and Courts have used a similar formulation.

Other scholars, such as Dan Solove, avoid this definition, arguing that it is too narrow and vague. While I don’t disagree with Solove’s concerns, I hope I avoid or mitigate them by the way I use this definition. First, my focus is much narrower than Solove’s. I am looking specifically at police access to information, particularly information stored on computers and in networks. Other aspects which fit within the common meaning of the broad word privacy—such as the decisional privacy right to make fundamental decisions about one’s body, reproduction, or rearing of one’s children—are well outside the scope of this Article. The critique is also premature, because Solove is concerned more with theoretical conceptions of privacy, whereas at this point I am merely developing a working definition. My choice of this definition, for example, does not mean I have chosen to neglect other theoretical justifications for protecting privacy, such as to protect human dignity and autonomy above and beyond the mere right to control.

Another slippery set of definitions is the distinction between confidentiality, secrecy, data security/protection and other terms synonymous with or related to privacy. Although I plan to develop these distinctions with some depth later, it suffices for now to say that I am concerned *both* with secrecy and some aspects of security. In particular, I am focusing on two separate risks to information privacy: surveillance, the collection of information authored by or about an individual, and attribution, the connection of people to information. There are many other risks that I am intentionally omitting from my analysis, such as the harm flowing from breach of trust in the handling of confidential information.

² [Schwartz and Treanor, Michigan Law Review]

³ [Richards, Georgetown Law Journal]

DRAFT VERSION: PLEASE DO NOT CITE

democracy. To hear them tell it, the essence of the Republic is at risk if we let privacy continue to slip away.

The New Privacy writers have focused much of their energy on concerns about private, corporate data brokers rather than the government. They have moved the spotlight from Orwell's Big Brother to Kafka's convoluted bureaucracies.⁴ They worry almost exclusively about the cumulative decisions of the officious, relatively benign middle-managers at private companies who want to know more about you and me not to control us, but simply to sell us more widgets. Individually, we may not worry about these people, but taken together, this marketing bureaucracy shifts power, and harms not merely the individuals, but the society as a whole.

The New Privacy movement scholars—with their diversity of views and approaches—seem to speak with one voice when compared to the messy crowd of scholars I have chosen to oppose them. This crowd includes nearly everyone else writing about privacy, more different than alike but tied together by two common traits: they tend to view privacy through the more traditional lens of rights and state interests, and their prescriptions tend to focus more on traditional utilitarian balancing tests and market-based conceptions of privacy. I'll call them the Balancers. These writers range from privacy-as-property market-driven libertarians,⁵ to Internet-Fourth Amendment scholars,⁶ to communitarians,⁷ to national security hawks.⁸

Although the New Privacy scholars have convinced many readers of privacy's deep values, they have very little to show for their labors. No new privacy legislation owes its existence to these writers, and no significant judicial opinion ties its logic closely to the societal rights identified by the movement. Presumably this critique matters to these writers, grounded as they are in a pragmatic view of the world,⁹ and dedicated to changing, not just commenting on, what they see as dire conditions.

⁴ [Solove, Stanford Law Review]

⁵ [Lessig, Stanford Law Review]

⁶ [Kerr, Michigan; Slobogin; Brenner]

⁷ [Etzioni]

⁸ [Stuntz; Posner]

⁹ [Solove, California Law Review]

DRAFT VERSION: PLEASE DO NOT CITE

Perhaps it is not fair to expect results from so young a movement—the earliest writings among these writers date to the middle-1990s, and some in the group didn't start writing until this century. Nevertheless, if past is prelude and the movement continues to fail to bring about practical change, there may be several explanations. First, even if these writers have convinced policymakers that privacy's values are important, the way they have framed these values comes across as vague and amorphous.¹⁰

Second, they tend to avoid any cost-benefits balancing. Their emphasis is almost always on the values of privacy or the concomitant harms from too little privacy, but very little attention is paid to the benefits on the other, security-protecting side of the scale. This tendency is not surprising, given the level of importance these writers place on privacy: once you've loaded so much weight onto one of the pans of the scale, what's the use of seeing what's sitting on the other side?

But what may ultimately doom the movement is its narrow choice of antagonist. They have chosen the private data broker over the public government agency; benign but officious bureaucrats over menacing spies and agents; and marketers over cops. They make these choices, they argue, because this is their point of novelty: we as a society underappreciate how much the private, commercial, data industry has caused us significant harm. But novelty is not the same thing as importance, and by focusing away from government harm, these writers seem strangely disengaged in the debates about NSA wiretapping, the war on terror, and government surveillance of networks. And given the events of this young century, the debates the movement has avoided are the debates where the most meaningful questions of information privacy are being addressed. The public and policymakers are concerned about data brokers, but not nearly as much as they are concerned about whether Al Qaeda operatives are using encryption.

Why have those in the movement spent so much time focusing on private databases and so little time on law enforcement access to personal information? Perhaps they simply don't care about Big Brother. Maybe the threat from private databases is not merely their principal concern, it is their only concern. This seems unlikely, because on a few occasions, these authors

¹⁰ [Richards, GEO. L.J.] (“[W]hile both policymakers and individuals share an unease about databases, privacy scholars have failed to articulate concretely the interests at stake in a way that has been broadly compelling to outsiders.”).

DRAFT VERSION: PLEASE DO NOT CITE

have focused on the law enforcement access question, and in this writing they have expressed a great unease at how government surveillance causes the same societal and individual harms as caused by private databases.¹¹

Second, maybe they take on *The Trial* rather than *Big Brother* because it is an easier foil. Although New Privacy writers tend not to spend much time balancing competing interests, implicit in their reasoning is a balancing which almost always weighs in their favor, because the competing interest is merely marketing. Perhaps the decision not to engage the law enforcement question betrays the fear that privacy's values are outweighed by crime or terrorist activity detection.

Third, perhaps the writers are simply tabling the law enforcement access question, choosing to tackle the easier (but still maddeningly vexing) question of private data brokers first before turning to look at law enforcement access. If this is true, given their seeming inability thus far to move the policy debate, one wonders if the harder government surveillance question will and can ever be addressed on their terms.

Also, if these writers are bracketing the discussion, they should say so. What they tend to do now is more like capitulation. When writing about private party access to data these authors will often drop a paragraph or two acknowledging the special problem of law enforcement access. In these paragraphs, they will usually acknowledge important countervailing law enforcement interests, and they will often concede that these competing interests outweigh privacy's interests in some cases. Although they need to make this concession to be taken seriously, by giving this only the barest mention instead of a sustained analysis, they seriously undermine their deontological claims.

The Balancers, in the meantime, rarely if ever engage the New Privacy movement, to their great detriment. They tend to think about privacy only in a person-by-person, individualistic way. Does this person's interest in the finite amount of privacy he has lost outweigh the cost (unsolved crime, undetected terrorist plot) of refusing the government's search? Similarly, the market-centric Balancers point repeatedly to what is by now an unassailable, empirical fact: individuals are quite willing to trade privacy for small benefits.

¹¹ [Solove.]

DRAFT VERSION: PLEASE DO NOT CITE

Even communitarians who would be expected to appreciate the New Privacy writers' claims to societal harms of invasions of privacy tend to focus only on the individual, and stack against her tiny individualistic claims of privacy the giant mass of nearly every evil in society.¹²

The basic problem is that these two sides aren't engaging one another. This doesn't seem to be a matter of benign neglect; it seems apparent that the two sides are simply unconvinced by one another's arguments. Granted, each side will often pay lip service to the other, being careful always to extol the virtues of the values described by the other side. "Privacy is indeed important," says the scholar about to urge for less of it, and "the need to protect our security is unquestionable," says her colleague, just before questioning it. One suspects, however, that neither side truly believes the other side's claims. There is an air of cordiality that needs to be stripped away, making the choices more starkly presented.

B. An Intractable Collision of Interests

There is no universally principled way to resolve the conflict between the irresistible force of security and the immovable object of privacy. At least as these fundamental concerns are explained by theorists, each side of the scale holds something so valuable, so dear, and so critical to our society, that shame on us if we are willing to sacrifice either one for the other.

The problem with this type of rhetoric is for those of us who sincerely believe the claims made by *both* sides. Security is an important goal, and given the fear—rational or not—we experience when thinking about terrorism, we hope the government can think of new ways to defend us from future attacks, and we're probably willing to give up some privacy for greater security. But we also agree with at least the spirit of the New Privacy scholar's descriptive and normative claims about privacy, valuing our privacy deeply and believing claims about the importance of privacy for self-determination, autonomy, and maybe even the loftier claims about the impact of privacy on deliberative democracy. Furthermore, recent experience teaches that balancing away those interests in the face of some security threat has proven too easy to do, and one wonders whether we can change the terms of the debate to better respect the values of privacy.

¹² [Etzioni.]

DRAFT VERSION: PLEASE DO NOT CITE

Those of us in the middle aren't persuaded by attempts to downplay either side's interests, and we think that both sides have made convincing claims of important value. Perhaps we're here because of our politics or philosophy, or because our institutional role (in the case of judges) compels a neutral disposition. But here we are, and largely because the two sides refuse to engage one another, the current scholarly debate doesn't seem to lend us the tools we need to translate our felt values into workable rules.

C. A Rhetorical Drag Race

Moving from the philosophy to the rhetoric used in the debate, the proponents of the value of each side are locked in a rhetorical drag race, each side responding to increased claims of importance (or more graphic descriptions of the harm that will result if their interest has to be sacrificed) from the other with an uptick in rhetoric. Those urging that security concerns trump privacy (generally or in specific cases) tend to the empiric, painting pictures of gloom and doom, pointing to 9/11, 3/11 and attacks in Britain as possibly avoidable if only there were less privacy.

On the other hand, those who feel privacy concerns are undervalued tend less to the empiric but instead reach for moral philosophy, weaving abstract theoretical examples of the harm we cause by diminishing privacy.

If you find yourself locked in an interest-balancing contest, there are three obvious strategies you can try, and the proponents in the privacy-security debate routinely try all three. First, you can play up your side's interest; second, you can denigrate or depreciate the other side's interest; and third, you can acknowledge the other side's interest but argue that the change proposed (to the law or technology) does not serve the interest well.

The New Privacy scholars focus in particular on the first strategy in several ways. First, they've tried simply to increase the importance of privacy's interests, declaring the loss of privacy the source of an entire host of societal ills. One reason they've chosen this approach is to mirror—but not address—the concerns from the other side. Before these scholars began writing, privacy had traditionally been framed as an individual interest while security has always been seen as a concern for all of society. The New Privacy scholars understood that by framing things in the traditional way, the individual interest, no matter how profound, was likely

DRAFT VERSION: PLEASE DO NOT CITE

outweighed by the collective concern.¹³ Julie Cohen and Paul Schwartz, in particular, have persuasively argued that the harms caused by the creation, use, and sharing of massive databases of personal information harm us collectively.¹⁴

Second, these scholars have tried to Constitutionalize information privacy's interests, to elevate them above merely ordinary concerns. Of course, viewing privacy as a Constitutional guarantee isn't novel. What is novel is where in the Constitution these scholars have found privacy. Traditionally, Constitutional talk about information privacy centered on the Fourth and Fifth Amendments protection against self-incrimination. Lately, these authors have tested the waters elsewhere in the Bill of Rights, discussing the effect of privacy invasions on due process, equal protection,¹⁵ and the First Amendment's guarantees of freedom of speech¹⁶ and freedom of association.

The second approach used in the debate is to dismiss part or all of one side's arguments, to suggest that the terror threat is exaggerated and overblown, or to assert that the harms of less privacy are overstated.¹⁷ Richard Posner, for example, has often questioned the values of privacy.¹⁸

The "interest depreciation" approach is taken much less frequently by the New Privacy scholars, who no doubt find it difficult to try to diminish the importance of security. Instead of making this move, these scholars tend to focus on the third approach, shifting attention away from the ends—security—and attacking instead the specific privacy-diminishing means proposed to further security. Data mining, in particular, bears the brunt of this critique, a symbol

¹³ Aleinikoff argues, however, that characterizing interests as private or public is "arbitrary," since most interests can be framed as both. [at 981] As an example, he discusses the interests weighed in *Hudson v. Palmer*, 468 U.S. 517 (1985), involving a search of a jail cell. Although the Court characterized the conflict as "between the prisoner's Fourth Amendment interest in privacy and the government's interest in jail security"—between an individual and a societal interest—the Court instead could have cast the prisoner's interest as public and societal. "Society has a general interest in preventing unwarranted governmental intrusions. Extending the Fourth Amendment's protection of privacy in one context may contribute to, and reinforce, a social sense of personal freedom and liberty. As a collective body, we are in the cell with Palmer; the interests at stake are not his alone." [Aleinikoff at 981] Similarly, the governmental interest could have been recast as private, focusing on the guards' "individualized interest in being free from assaults and in having a governmental authority protect them." [Aleinikoff at 981.]

¹⁴ [Cohen] [Schwartz].

¹⁵ [Solove in *Chi L Rev*] [Slobogin in *Chi L Rev*]

¹⁶ [Solove's Fourth/First Amendment]

¹⁷ [Aleinikoff at 975] ("Another technique is to depreciate the value of one of the interests at stake.").

¹⁸ [Posner/Georgia.]

DRAFT VERSION: PLEASE DO NOT CITE

of a futile attempt to protect the homeland, and accordingly a bad trade-off for the amount of privacy it reduces.¹⁹

None of these approaches helps us determine whether privacy or security should prevail in any particular case. With automobile drag races, even when you can tell who has won, what you're really left with is the impression that both cars were very fast. Similarly, both of the dragsters in this race are fast—we believe in each side's compelling claims of value—but we really can't tell which one should win.

There is another reason why this debate suffers from the drag race mentality, and this problem can be fixed: we have trouble deciding whether privacy or security should prevail in any given situation, because we haven't taken advantage of the legal tools needed to do that balancing.

II. Poor Tools for Balancing

A. The Wrong Tools for Balancing

For those of us who see some truth in both sides of the privacy and security debate, we are left almost unaided by the rhetoric. If both sides have points to make, and because both sides phrase things in such absolute terms, there isn't a principled way to choose between the competing values, in a case-by-case basis.

With little help from an intractable scholarly debate, policymakers seem to make decisions in an ad hoc, unprincipled manner. Sometimes security is sacrificed, not because it is “outweighed” by privacy concerns, but because the privacy concerns are simplistically and artificially elevated, often in response to a particularly salient and available anecdote. So, the Video Protection Privacy Act and the Driver's Protection Privacy Act were enacted to limit access to records relating to video rentals and driver's licenses, respectively, because Judge Bork and Rebecca Schaeffer were politically expedient stand-ins for privacy interests.²⁰

More often, however, the side that loses out is the privacy protecting side, seeing their more abstract discussions of privacy's values being swept aside in the face of horrific images or

¹⁹ [Solove.]

²⁰ [Zittrain/Stanford (near FN119-122)]

DRAFT VERSION: PLEASE DO NOT CITE

stories of attack and carnage. So 9/11 begat the USA PATRIOT Act and the NSA Warrantless Wiretapping program.

To be sure, in all of these examples—save the NSA Wiretapping perhaps—lawmakers engaged in a kabuki dance of weighing the necessity of invading privacy with the values of privacy that are invaded. In cases like these, legislators make arguments about the relevant weight to give to different categories of privacy—telephone call content is more private than numbers dialed which is more private than the home address you’ve registered with your phone company. In this sense, they are hoping to appear to be minutely calibrating this very difficult balance. But this balance is impossible to make if you believe the claims of value put forth by scholars: if the privacy maximizers are correct and the essence of our democracy is at stake, measuring the relative worth of different types of privacy seems illogical. Similarly, if the only way to protect us from terrorists is to give up some privacy, then balancing is a waste of time.

The problem with balancing two equally important and seemingly unmoving interests is that anytime one side prevails on any narrow set of facts, the other side—engaged as it were in a game of brinksmanship—views the result as a loss. This is the “Thunderdome” approach to balancing, a zero-sum endeavor where two opposing principles enter, and only one can emerge victorious.²¹

B. The Problem with Law Enforcement Exceptions

To be more specific about it, when New Privacy writers move from theory to practical application, they tend to peg their hopes on legislatures not courts.²² Sometimes, they’ll even

²¹ MAD MAX BEYOND THUNDERDOME, Warner Bros. (1985) (“Two men enter, one man leaves.”). Beyond Thunderdome has become a bit of a meme in legal scholarship. See Comment, Zachery Z. Annable, *Beyond the Thunderdome—The Search for a New Paradigm of Modern Dispute Resolution: The Advent of Collaborative Lawyering and its Conformity with the Model Rules of Professional Conduct*, 29 J. Legal Prof. 157 (2004-2005) (“The post-apocalyptic setting of the Thunderdome is eerily analogous to the modern courtroom; one can almost hear the bloodthirsty crowd chanting, “[t]wo men enter, one man leaves,” as today’s litigators prepare to do battle.”); Alex Kozinski, *How I Narrowly Escaped Insanity*, 48 UCLA L. Rev. 1293 (2001) (calling *Thunderdome*, “one of my favorite law-related movies”).

Judge Kozinski quipped in his article/speech that the fictional town in Thunderdome, Bartertown, also has one law of contracts: Bust a Deal, Face the Wheel. I have heard Eugene Volokh, ex-Kozinski clerk, make a similar quip on more than one occasion.

²² [Schwartz, *New Privacy*, near end.]

DRAFT VERSION: PLEASE DO NOT CITE

draft model statutes²³ or point to the data privacy directive in Europe.²⁴ In any of these cases, with their unwavering focus on private actors—huge corporations with massive databases—the way they deal with *law enforcement* needs is by throwing in an exception. These exceptions suffer from a problem of extremes. They either make it so difficult for law enforcement officials to do their jobs as to be politically unsaleable or they are so sweeping and deferential to law enforcement that they swallow the rule.

An example of an overly restrictive law enforcement exception was proposed by Jerry Kang, as part of a model act which would prohibit data possessors from doing any data processing on personal information that wasn't "functionally necessary," unless the data subjects opted in.²⁵ This act would, in effect, deny many private data collectors much of the freedom to use and redistribute personal information they enjoy today, and in some ways is along the lines of the solutions proposed by the New Privacy scholars. But on the law enforcement access question, admittedly not the focus of Kang's discussion, his model act contains an exceptionally narrow law enforcement disclosure exception, giving the police access to the data only if they give the subscriber both notice and an opportunity to contest the police claims.²⁶

[Talk about over-deferential LE exception such as in Solove/Hoofnagle.]

C. The Problem with Justification Standards

The worst thing about the way scholars and legislators write law enforcement exceptions is how they stick so closely and unimaginatively to the approaches of the past. Most scholars in this field focus entirely on one requirement in law, the justification standard—the amount of suspicion the police need to claim to possess before they can invade the protected privacy interest—as the sole method for regulating police access to information.

There's a pedigree to the justification standard method for regulating privacy and security. It's practically Constitutional dogma that the distinctions between probable cause, reasonable suspicion, and mere relevance are meaningful, and that given any particular case, a police officer faced with a probable cause requirement is likely to behave differently than an

²³ [Kang.]

²⁴ [Schwartz.]

²⁵ [Kang.]

²⁶ *Id.* at 1292 (Proposed Cyberspace Privacy Act § 6).

DRAFT VERSION: PLEASE DO NOT CITE

officer needing to show reasonable suspicion. *Terry v. Ohio*—which held that the police could conduct brief stop and frisk interrogations upon less than probable cause—is the Constitutional lode star for this understanding, and some have described statutes that allow police access to information in the absence of probable cause as “*Terry* stops for e-mail.”²⁷

I want to challenge this Constitutional dogma or at least argue that it doesn’t translate well to questions of information privacy, and I will argue that scholars should be looking at other ways to regulate police behavior. Some of these critiques would appear to apply outside information privacy, and perhaps even cast some doubt on the force of *Terry*’s logic—but that’s a topic for another article.

Let us focus first on the top two tiers, probable cause and reasonable suspicion. Is the difference between probable cause and reasonable suspicion as meaningful as courts and commentators have assumed?²⁸ What is the difference between the two standards? Notice first what the two standards share in common: both focus exclusively on one question—what has this particular police officer already uncovered or already know about this person, evidence, or event? Notice also what neither standard asks, what have the police already done? In other words, the standards focus only on what the police *know* or can *infer*, not on what they have *done*. The standards measure present, mental knowledge, and not past, physical action.

This is where I think the commentators and Congress have misread *Terry*. In departing from the venerable probable cause standard, the Supreme Court wasn’t really that concerned with the grounds for Officer McFadden’s suspicion. The Court spent a little time discussing what piqued the Officer’s suspicion—the suspects’ furtive pacing, the oddly repetitive routine—but they spend more time on the exigency of the situation, the fact that McFadden didn’t have time to go find a judge. This case wasn’t about the Officer’s intellect and deductive reasoning or persuasive affidavit writing ability, but instead, it was about very different human virtues—instinct, experience, and intuition. Chief Justice Warren’s retelling of the facts of that fall day in Cleveland are words about action not logic:

²⁷ [Slobogin, Transaction Surveillance by the Government., 75 Miss. L. J. at 163]

²⁸ [Slobogin’s Chicago Symposium piece footnotes earlier work defining and pegging those standards.]

DRAFT VERSION: PLEASE DO NOT CITE

His interest aroused, Officer McFadden took up a post of observation in the entrance to a store 300 to 400 feet away from the two men. . . . He saw one of the men leave the other one and walk southwest on Huron Road, past some stores. The men paused for a moment and looked in a store window, then walked on a short distance, turned around and walked back toward the corner, pausing once again to look in the same store window. . . . The two men repeated this ritual alternately between five and six times apiece—in all, roughly a dozen trips. . . . Deciding that the situation was ripe for direct action, Officer McFadden approached the three men, identified himself as a police officer and asked for their names. . . . When the men ‘mumbled something’ in response to his inquiries, Officer McFadden grabbed petitioner Terry, spun him around so that they were facing the other two . . . and patted down the outside of his clothing. In the left breast pocket of Terry’s overcoat Officer McFadden felt a pistol.

Terry is about the exigencies of street-level police work and about the need for quick action in that environment. All of these important factors are lost by the time the *Terry* stop-and-frisk becomes a *Terry* order for e-mail. In the e-mail context, stripped of any exigencies, the need to act without a neutral magistrate, and the police work-in-action, all that’s left are the words—reasonable suspicion—and we make too much of those words if we presume that they refer to a much lower hurdle than probable cause.

Second, even though these standards are thought to embody Congress’ careful *balancing* of the competing interests, neither standard turns at all on the privacy interests at stake. Neither one asks the police to articulate or justify why their interests outweigh the privacy interest. Instead, we assume Congress did that balancing once and for all when it passed the statute, carefully calibrating the various privacy interests and reflecting that calibration by pegging access to a particular type of information to a particular standard. But once Congress has made this initial sorting, no police officer needs to think about particular sensitivities or privacy concerns.

Obviously, the thought that Congress could fine-tune the balance just right, sensitive to changing technologies and public attitudes is far-fetched. It would be better if Congress

DRAFT VERSION: PLEASE DO NOT CITE

sketched the basic contours of privacy law, leaving the detailed, specific balancing to police officers and, ultimately, to judges.

Third, the police are less likely to worry about the justification standard if a statute fails to offer the person aggrieved incentives or mechanisms for challenging the search. The Stored Communications Act, for example, carves out an elaborate warren of varying suspicion standards, requiring the police to assert probable cause in some cases, clear and articulable relevance and materiality in others, mere relevance in a third, and sometimes nothing at all, for access to online information. But the SCA does not provide a suppression remedy for violations.²⁹

Orin Kerr has criticized this shortcoming in the SCA for failing to give criminal defendants an incentive to challenge the law, meaning fewer judicial opinions interpreting the statute, leading to murky, unpredictable rules.³⁰ Similarly, one wonders how a lack of suppression affects police incentives. Are the police as likely to worry about whether their facts cross the illusive line between probable cause and reasonable suspicion, if they are allowed to use the evidence even if they are wrong?

Thus, justification standards are clumsy tools for balancing security and privacy. They ignore the privacy side of the balance; they're toothless if not backed by suppression remedies; and instead of searching inquiry, they're usually given cursory review. The image of the police officer who is asked to meet a justification standard is an officer sitting at his desk, pecking away at a word processor, trying to explain why he suspects what he suspects. The hurdles placed in the officer's way are merely administrative, involving paperwork and bureaucracy. Wouldn't it be better to find regulatory tools that invoke the image of the police officer in action, tracking leads, testing theories, and evading detection before crossing the next line of privacy?

The claim that the line between probable cause and reasonable suspicion is illusory is supported by a natural experiment set up in the wake of a 2004 Ninth Circuit opinion, *Theofel v. Farey-Jones*.³¹ *Theofel* arose from a civil discovery request in commercial litigation. The defendant to the litigation sent a trial subpoena to the plaintiff's non-litigant ISP. The subpoena

²⁹ [Kerr, Hastings.]

³⁰ *Id.* at xxx.

³¹ 359 F.3d 1066 (2004).

DRAFT VERSION: PLEASE DO NOT CITE

was broad, asking the company to produce “[a]ll copies of e-mails sent or received by anyone” at the plaintiff.³² Writing for the unanimous three-judge panel, Judge Kozinski agreed with lower court judges that the subpoena was “transparently and egregiously” in violation of Federal Rules. After the ISP complied, in part, with the subpoena some of the users whose e-mail messages had been disclosed sued, claiming violations of the Stored Communications Act, Wiretap Act, and Computer Fraud and Abuse Act.

The question which arose was, does the release of e-mail messages in response to this kind of trial subpoena comply with the federal SCA? Judge Kozinski said no,³³ inadvertently wading into law enforcement’s interpretation of the SCA. Not only does the SCA provide civil remedies for subscribers wronged by their ISPs, the SCA regulates whether law enforcement can access stored e-mail messages. And the same exact definitions apply in both contexts, so when a Judge opts for a privacy-protective interpretation in a civil case against an ISP, it also, usually inadvertently, creates a new privacy hurdle for law enforcement.

In this case, the Department of Justice had long interpreted the SCA to make a distinction between some types of e-mail messages (those stored by an ISP in “temporary, intermediate storage”) which could be obtained only with a probable cause warrant and other types of e-mail messages (those stored for other reasons) which could be obtained with a particular kind of

³² *Id.* at 1072, 74.

³³ *Id.* at 1073.

DRAFT VERSION: PLEASE DO NOT CITE

reasonable suspicion order.³⁴ Judge Kozinski’s interpretation would all but read the latter category out of the statute,³⁵ forcing DOJ to get a warrant to obtain any stored e-mail messages.

In response to an amicus brief by DOJ, Judge Kozinski amended the opinion, reaffirming the holding.³⁶ The amended opinion explicitly rejected DOJ’s interpretation. *Theofel* thus rejected DOJ’s interpretation of a nearly two-decades old statute and conflicted with numerous training manuals³⁷ and other written publications.³⁸ Virtually overnight, the ground rules for law enforcement access to stored e-mail messages had changed from a reasonable suspicion to a probable cause standard.

Longtime DOJ-watchers made confident predictions about what would happen next, based on years of past experience. For, in the field of online surveillance and online crime, DOJ had proved repeatedly that after adverse decisions, the road from the courthouse to Congress was very short. In the past, in the face of any judicial opinion—even from a magistrate judge—which could be portrayed as making DOJ’s job harder to do, DOJ had lobbied Congress for an amendment. Less than a year after a magistrate judge ruled that warrants under the SCA had to be served in person and not by fax machine in *United States v. Bach*,³⁹ Congress amended

³⁴ [S&S Manual]. The order is found in 18 U.S.C. § 2703(d) and is therefore often referred to as a “2703(d) order” or simply “D order”. 2703(d) provides, in pertinent part:

(d) **Requirements for Court Order.**— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers *specific and articulable facts* showing that there are *reasonable grounds to believe* that the contents of a wire or electronic communication, or the records or other information sought, *are relevant and material* to an ongoing criminal investigation.

18 U.S.C. 2703(d) (emphasis added). Note that D orders are not simply reasonable suspicion orders. Although the order requires “reasonable grounds to believe,” they require “specific and articulable facts,” and the “belief” must be that the information sought is “relevant and material” to the investigation. In some ways, this is a more stringent standard than the Terry stop standard—for example, Terry doesn’t require “specific and articulable facts.” On the other hand, some have argued that the D Order standard is easier to meet, because unlike Terry, where the suspicion must involve “a targeted individual,” a D Order allows records relating to the investigation, even if not directly related to an individual. [Slobogin, Mississippi], 161.

³⁵ All but read out, but not read out entirely. In response to DOJ’s argument that *Theofel* would “read out” the part of the statute which required reasonable suspicion orders, Judge Kozinski explained that ISPs that provide only “storage or computing processing services” would still be amenable to process under the reasonable suspicion order provision.

³⁶ *Id.* at 1077 (“We acknowledge that our interpretation of the Act differs from the government’s and do not lightly conclude that the government’s reading is erroneous.”).

³⁷ [S&S Manual.]

³⁸ [USAM?]

³⁹ *United States v. Bach*, []

DRAFT VERSION: PLEASE DO NOT CITE

the SCA to make it clear that service-by-fax was allowed.⁴⁰ When magistrate judges refused to honor warrants for e-mail issued from out of their district, Congress amended the SCA to provide for nationwide service of process.⁴¹ After a few appellate courts ruled that stored voice mail messages were protected by stricter privacy controls than stored e-mail messages, Congress fixed the problem.⁴² The latter two provisions—floated for several years and included in several proposed bills—passed finally in the USA PATRIOT Act.

Similarly, with substantive computer crime law, DOJ has had great success legislatively overturning several opinions with which they disagreed. In response to *United States v. Morris*,⁴³ the first notorious computer virus case, Congress amended the Computer Fraud and Abuse Act to deal with tricky questions about authorization that the case had spotlighted.⁴⁴ In response to *United States v. LaMacchia*,⁴⁵ Congress passed the No Electronic Theft Act, to allow criminal copyright convictions even when the perpetrator lacks a profit motive.⁴⁶ In response to *United States v. Czubinski*,⁴⁷ Congress added a section to the CFAA criminalizing obtaining information from a computer with the intent to defraud.⁴⁸

In all of these past cases DOJ had related its wishes not only privately in the offices of Congressional members and staffers but also publicly in the Senate and House hearing rooms. DOJ Deputy Assistant Attorney Generals have a long history of carping about recent judicial affronts nearly any time they are asked to brief a Senate or House committee or subcommittee on any topic involving computer crime.⁴⁹

⁴⁰ 18 U.S.C. § 2703(g) provides,

(g) Presence of Officer Not Required. — Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

⁴¹ [Ohm, George Washington L Rev.] [USA PATRIOT Section 220.]

⁴² [USA PATRIOT 209].

⁴³ [Morris]

⁴⁴ [Cite for public law which made amendment; cite for 1030 provision].

⁴⁵ [LaMacchia]

⁴⁶ [Cite for public law which made amendment; cite for 1030 provision].

⁴⁷ [Czubinski]

⁴⁸ [Cite for public law which made amendment; cite for 1030 provision].

⁴⁹ [Long string cite.]

DRAFT VERSION: PLEASE DO NOT CITE

This history is meant to prove a point: we would have expected DOJ to aggressively direct its influence on Capitol Hill to overturning *Theofel*. If DOJ was willing to knock on legislators' doors to protect the right of FBI agents to use fax machines, how much more motivated must DOJ have felt to overturn a ruling which required probable cause instead of reasonable suspicion before any law enforcement agent in nine states in the Western U.S. (including the home states of Yahoo!, MSN Hotmail, and Google) could access stored e-mail? Of course, this assumes that the difference between reasonable suspicion and probable cause is as important as it's assumed to be.

But the expected bang hasn't even been a whimper. No DOJ official has ever mentioned the *Theofel* case in public testimony. No legislation has ever been introduced which would overturn *Theofel*. A search of the entire usdoj.gov site for references to *Theofel* returns two paragraphs in a recent manual on prosecuting cybercrime, in which a DOJ subcomponent offers, a bit meekly, "[The Computer Crime and Intellectual Property Section] continues to question whether *Theofel* was correctly decided"

Of course, with an organization as large and complex as DOJ it is hard to draw absolute conclusions from the decision not to lobby Congress. Perhaps there were reasons—political or otherwise—that militated against trying to “fix” *Theofel*. But DOJ's inaction strongly suggests that the difference between probable cause and reasonable suspicion isn't all that it's been cracked up to be, at least not when it comes to online investigations and information privacy.

So far, I have focused on the difference between probable cause and reasonable suspicion. This leaves the category of mere relevance. Under many of the information privacy statutes, police access is allowed once the police prove or assert that the information sought is relevant to an investigation. This is also the standard for a grand jury subpoena, so in that sense, relevance is the default standard, applicable whenever the police want to compel a person to produce information in any of the myriad situations where a privacy statute doesn't apply.

Unlike the non-distinction between probable cause and reasonable suspicion, the difference between either of those two standards and mere relevance is almost certainly meaningful. Relevance has been defined in cases involving motions to quash grand jury

DRAFT VERSION: PLEASE DO NOT CITE

subpoenas as an exceptionally low standard.⁵⁰ Because of the necessarily speculative mission of the grand jury, the Supreme Court defined the standard as exceedingly low: “where, as here, a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.”⁵¹ In another part of the same opinion, the Court seems to imply that all that the standard does is ensure that police are “not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or an intent to harass.”⁵² With this low a hurdle, it seems certain that probable cause and reasonable suspicion—however you define those standards—is qualitatively different than the relevancy requirement.

III. What Lies Between Privacy and Security: Investigative Friction

A. Friction

It is often said that in the real world, cash provides perfect anonymity, but of course it does not. Cash has benefits for privacy and burdens on security, but it doles out these costs and benefits in not unlimited ways. If a criminal buys the tools or materials he needs to commit his crime (bomb-making materials, child pornography, fuel for his getaway car) with cash, he will be much harder but not impossible to trace. The bomb-maker might have left behind a signature on a contract for purchase of parts, the child pornography purchaser might be a repeat customer, and the getaway driver might have had his image captured on a surveillance camera. Most importantly, all three had to hand their cash, face-to-face, to a cashier.

To the police, cash is what I call investigative friction. It makes a crime much more difficult to solve. Along the privacy-security spectrum, it pushes toward the privacy end, but it doesn’t take either side out of the game. The criminal may yet get away with the crime, and the cop may yet find his quarry. There is great virtue to friction, and we should abandon calls for absolutist solutions and should instead look for ways to inject friction back into the system.

⁵⁰ *United States v. R. Enterprises*, 498 U.S. 292 (1991).

⁵¹ *Id.* at 301.

⁵² *Id.* at 299.

DRAFT VERSION: PLEASE DO NOT CITE

The amount of friction can of course vary, and at this stage in the analysis, I am not trying to decide how much is enough. I will return to that question in a later section, but the more important point is that some friction is the best way to finely calibrate the power relationship between the government and criminal targets.

B. Frictional Law Enforcement Exceptions

As I argued in Part II, justification standards aren't all they're cracked up to be. The difference between probable cause and reasonable suspicion is not as important a distinction as many seem to believe.

Although, as I acknowledged in Part II, the distinction between probable cause (or reasonable suspicion) and mere relevance probably is important, there is good reason to believe that there are only two meaningful rungs in the ladder. The first is the step from “no justification required” to “mere relevance” and the second is the step from “mere relevance” to “something more,” with both probable cause and reasonable suspicion falling in the last category.

This observation calls into doubt solutions of pure proportionality. Chris Slobogin, for example, has argued that what is needed are even more intermediate justification standards between probable cause and mere relevance, along with a graduated scale of investigatory methods, tying the standards in the first list to the methods in the second.⁵³ I doubt that such an exercise would lead to meaningful distinctions. Once you're at mere relevance, you've abolished pure fishing expeditions. Once you're at any stage beyond mere relevance, you've abolished true long shots. It is hard to believe that judges will be able to parse justification standards any more finely than that in a meaningful way.

Rather than invest energy in formulating new justification standards, there are other ways to change procedural law to better introduce investigative friction. Again, at this point I'm not urging for any or all of these particular changes in any particular law; instead, I'm trying to point to an arsenal of changes that might lead to a “third way” in privacy/security debates.

⁵³ [Slobogin, St. John's]

DRAFT VERSION: PLEASE DO NOT CITE

1. Prioritization

First, legal rules can be used to force the police to use certain investigative techniques in a particular order. The theory is that some steps are so privacy-invading, police officers should not be allowed to take them until they have tried less-privacy-invading steps and failed. So, we might use prioritization to require the police to stake out a house before they pull trash, and to pull trash before they install a phone wiretap.

Prioritization is rarely seen in legislation, but it takes one especially aggressive form: wiretap law's necessity requirement. Necessity is both a Constitutional and statutory⁵⁴ mandate. According to the federal law, a police officer applying for a wiretap must include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous," and the judge must determine based on the facts that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." This is no rubber stamp; Congress has given the judge the power to conduct a searching review of necessity.

Notice the connection between necessity requirements and justification standards. Both focus on how far along the police are in their investigation. But they measure this in different ways. Justification standards ask, what do you think you can prove at this point in time? They focus on the police officer's ability to articulate his best case for pushing ahead to the next, more privacy-invading step in the investigation.

Necessity requirements ask a different question: what else have you done? It doesn't matter what the police know or how well the police can write. I argue that this is what the justification standards really are trying to get at, but in a much more direct way. Congress uses justification standards to rank order our privacy interests. Wiretapping violates our privacy the most, access to e-mail is next and non-content monitoring is third, one could argue Congress to be saying. Thus, by carefully calibrating justification standards, we'd expect non-content monitoring to occur in most investigations before access to e-mail, which should usually precede wiretapping. But if that's what Congress has been trying to do implicitly, they should just do it

⁵⁴ *Id.*

DRAFT VERSION: PLEASE DO NOT CITE

explicitly, with necessity requirements, especially because, as I argued in Part II, the difference between probable cause and reasonable suspicion is illusory.

Justification standards reward time spent at the word processor or, worse, time spent modifying boiler plate. It doesn't correctly value privacy, and given my arguments in Part II, it may not value privacy at all. Necessity requirements, in contrast, go more to the heart of the matter. In the few cases where necessity has been written into the law, Congress and the courts wanted the police to do things like video surveillance and wiretapping last, because these things are so privacy invasive that they merit a different prioritization.

2. Tailoring

Investigative friction also arises by forcing the police to tailor the use or disclosure of the information they gather. The classic example is wiretap's statutory and Constitutional minimization requirements. To satisfy minimization, the police must use controls to limit the communications they intercept to those relevant to the investigation. There are two styles of minimization, and the "new style" doesn't generate as much investigative friction as the old. Old style minimization was used for decades for analog telephone line wiretaps, and it can still be seen depicted in old cop movies and the television show, *The Wire*. Old style minimization requires the police to listen to each new call for a set amount of time—specified in the wiretap order—and if nothing relevant is heard, they must hang up the line for another set amount of time, or until the call ends.

Suppose the police are obligated to use a two minutes-on, four minutes-off minimization routine. This means that up to two-thirds of the conversations that aren't immediately relevant are presumed irrelevant, and for privacy reasons, they are not intercepted. Obviously, this can frustrate law enforcement goals. If two-thirds of the conversations are not captured, perhaps the most important clues are being missed. The point, however, is investigative friction. This type of minimization slices up the clock like a pie chart, with one wedge labeled "security," and the rest of the circle labeled "privacy."

New-style minimization restricts the police less. For e-mail or Internet traffic wiretaps, the police typically get judicial authorization to collect and store everything. They then minimize by repeatedly running keyword searches against the data collected. Although practices

DRAFT VERSION: PLEASE DO NOT CITE

probably vary, one imagines that the keywords aren't even specified in the initial application, because the attesting agent can argue that the list of keywords will evolve as the monitoring progresses. ("We didn't know about the important phrase, 'Morpheus believes he is the one,' until the third day of monitoring."). With old-style minimization, those old conversations would have been lost. With new-style minimization, the police may get many bites at the apple.

Of course, even with new-style minimization, it is likely that some relevant evidence is lost. Even new-style minimization is still a form of investigative friction. This highlights the fact that investigative friction spans a spectrum of possibilities, with some closer to the security side, and others nearer the privacy side of the balance.

3. Oversight

Third, laws can impose more oversight. The principal type of oversight is judicial. Of course, the amount of judicial friction will vary, depending on the discretion and scope of review afforded the judge. Under federal law, the pen register or trap and trace act and USA PATRIOT Act Section 215 both seem to strip judges of almost all discretion. Section 3123(a)(1) provides:

Upon an application made under section 3122 (a)(1), the court *shall enter* an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, *if the court finds that the attorney for the Government has certified* to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.⁵⁵

While USA PATRIOT Act Section 215 provides:

Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.⁵⁶

Simply requiring officers to take a trip to the courthouse on their way to the third-party record holder isn't meaningful unless the judge is given at least some discretion to scrutinize and reject the application.

⁵⁵ 18 U.S.C. § 3123(a)(1) (emphasis added).

⁵⁶ 50 U.S.C. § 501(c)(1).

DRAFT VERSION: PLEASE DO NOT CITE

Oversight need not come from only the judiciary. Sometimes, intra-branch or intra-agency oversight can be a powerful limiting factor. As I have explored in an earlier article,⁵⁷ the federal Wiretap Act pits two subcomponents of the Department of Justice against one another, by using the same language to regulate both police officers and ordinary citizens who want to wiretap. Aggressive interpretations of the statute by investigators who want to wiretap will mean that those aggressive interpretations may make it more difficult to prosecute civilian wiretappers in the future. This kind of “parallel effect” statute can engender intra-agency debate and will often lead, I have argued, to moderate interpretations.

Intra-agency and intra-branch oversight can also be even more explicit. For example, by statute and regulation, any requests for foreign intelligence surveillance under FISA must be approved first by DOJ’s Office of Intelligence Policy and Review. OIPR is well-known within DOJ as a careful, meticulous agency who does not rubber-stamp applications, and FBI agents sometimes grumble that the real hurdle to getting a FISA order is DOJ not the FISA court.

4. Accountability

A final legal source of investigative friction is increased accountability. Accountability can be increased, for example, by requiring the FBI to make reports to Congress. Accountability works *ex post*, by shining a light on internal police practices. But accountability can also work *ex ante*, as investigative friction. If wiretapping must be reported to Congress at the end of the year but trash pulls need not, the police may choose to engage in the latter more often and the former less often.

Another form of accountability is tied closely to justification standards. Some statutes require “clear and convincing evidence” of whatever level of proof is required.⁵⁸ Similarly, the SCA requires “specific and articulable facts” before a court will issue a specific type of order called a 2703(d) order. Sometimes, these phrases are referred to as justification standards, but they aren’t. They are simply mechanisms for increasing accountability and making oversight more meaningful.

⁵⁷ [Ohm, *George Washington L Rev*]

⁵⁸ *See, e.g.*, Bail Reform Act of 1984, 18 U.S.C. § 3142(f) (requiring proof by clear and convincing evidence that “no condition or combination of conditions will reasonably assure the safety of any other person and the community.”).

DRAFT VERSION: PLEASE DO NOT CITE

IV. How Much Friction? “Good Enough” Privacy

A. How Much Friction?

The principal claim I have made thus far is that we will have a more meaningful, more transparent debate about security and privacy if we stop thinking of “balance” as a winner-take-all, Thunderdome-style conflict and instead think of it as a careful setting of investigative friction. Of course, this simply redefines the debate, but it doesn’t resolve it. Privacy minimizers will argue for very little investigative friction and privacy maximizers will argue for a lot. At the extremes, friction looks a lot like zero-sum balancing, but the benefit of friction is it provides a vocabulary for finding compromise in between.

At this point, I choose sides. I agree with the privacy maximizers, the New Privacy scholars, that privacy is undervalued in current debates. I make this claim by focusing less on the deontological harms that results when e-mail messages are handed over the police, and more instrumentally, by noting that the principal method for regulating privacy vis-à-vis the government is the statutory justification standard, which as I’ve argued, does not usefully contribute to the debate. Sure, Congress can distinguish between low-privacy and high-privacy interests, and give the police access to the former with a relevancy standard and the latter with some other, higher standard, but that’s all they can do. It’s simply not realistic to think that justification standards can be used any more granularly.

Therefore, Congress needs to introduce more investigative friction into the analysis, to require the police to work a little harder before they can access certain types of private information. Again, I’m not sure exactly where those lines should be drawn, but I believe that through the use of a few novel procedural requirements, Congress can shift the ball a little, or a lot, to the other side.

B. How Much Legal Friction?

Investigative friction can be built into laws much more effectively than with current attempts to tweak justification standards. In this part, I propose a few novel examples

DRAFT VERSION: PLEASE DO NOT CITE

1. Tiered Necessity

One way to force investigative friction is by introducing more necessity requirements into surveillance laws. This could add bite and enhance the privacy of particular types of information beyond what a merely enhanced justification standard can do.

But there is a logical problem with extending necessity to other laws. As it has been currently conceived, necessity means that agents must first try every other investigative procedure or explain why other procedures aren't likely to succeed.⁵⁹ As a logical matter, there can only be one investigative procedure with this form of necessity requirement, for how can you claim to have done everything if two of the possible investigative procedures both require that showing?

The simple solution is to require that the police have tried every other investigative procedure except procedures with necessity requirements of their own—let's call this "set necessity." So, for example, if installing a keylogger is made subject to a set necessity requirement, the police must demonstrate why they have tried every other investigative procedure except wiretapping. The problem is that as these necessity requirements proliferate, each new requirement will reduce the privileged placement of the others. When wiretapping is the only necessity requirement in the books, it is held in a privileged plane, above all other procedures. But if wiretapping is joined by ten other procedures (access to e-mail contents, spyware distribution, cell phone tracking, etc.) in a privileged "tier" then wiretapping can occur before any of its peers in the same set, making wiretapping a bit easier to justify.

The solution to this problem is to create multiple tiers, with procedures in a given tier inaccessible to police until they have satisfied the necessity requirement for all "subservient" tiers. I call this Tiered Necessity. For example, imagine the federal privacy statutes are amended to create these three tiers of Tiered Necessity.

1-Necessity: voice wiretapping, sneak-and-peek search, keylogger installation, spyware distribution.

⁵⁹ 18 U.S.C. § 2518 ([paren]).

DRAFT VERSION: PLEASE DO NOT CITE

2-Necessity: access to stored e-mail content, cell phone location tracking, automobile beeper tracking, video rental record access.

3-Necessity: pen-register, trap-and-trace, access to stored non-content relating to e-mail, some forms of data mining.

Within this hierarchy, 1-Necessity procedures are the procedures considered the most invasive to privacy, and each step down the hierarchy represents a decrease in privacy concerns. Thus, in order to access stored e-mail content, which is a “2-Necessity procedure,” the police need to provide “a full and complete statement as to whether or not other investigative procedures [in tier 3-Necessity and below] have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.”⁶⁰ So, the police will need to first try a pen register as well as access to stored non-content relating to e-mail. Also, any investigative procedure not assigned an n-Necessity tier will need to be tried or explained; for example, the police will need to tell the court about their past attempts to find a confederate, monitor the target visually, and pull his garbage.

One advantage of the tiered system is that the entire hierarchy need not (and should not) be created all at once, in one law. Instead, different procedures can be added to tiers one-at-a-time, giving legislators time carefully to compare and contrast the value of each procedure and the intrusiveness to privacy. This also allows Congress to categorize procedures with well understood costs and benefits today, but save the categorization of new techniques and technologies until they have more experience evaluating its use. Access to stored e-mail content is a well-understood police technique, but data mining is less well understood. Perhaps e-mail access can be categorized today while data mining could be left not subject to Tiered Necessity requirements until later.

There are many other advantages to this system. First, it causes Congress to balance security and privacy much more explicitly than they do now, by forcing them to compare each new regulated technique with past techniques they have considered. For example, if Congress

⁶⁰ 18 U.S.C. § 2518.

DRAFT VERSION: PLEASE DO NOT CITE

decides to regulate police access to cell phone location tracking data, in deciding which tier to place the technique, legislators will need to confront much more directly the invasiveness of cell phone tracking and the value to law enforcement. Contrast this with the current system of deciding which of three (or more) levels of justification is required for the technique, a process which is both less granular, and also a process in which the decision may not matter much to police.

Second, the police are comfortable with the idea of necessity requirements, at least those officers who have applied for wiretap orders.

Third, judges will find the tiers easy to apply. Rather than try to struggle with whether probable cause means 30%, 51% or 75% certainty,⁶¹ judges will simply need to look at the list of past procedures, the justification for procedures not tried, and compare them to the various statutes. Judges will also have much more insight into Congress' assessment of the security/privacy balance of a given technique. When faced with a complicated new technology, the judge will be able to compare the technique to other techniques in the shared tier to understand how Congress viewed the relative interests and concerns. For those who worry about activist judging, this will place a democratic constraint on judges.

One possible objection to Tiered Necessity is that it intrudes too much on police discretion or that it micro-manages the police. I disagree. Unless the hierarchy expands to include many tiers with many investigative techniques, the burden will probably be slight. All an officer needs to be given is a chart of the tiers and an explanation that procedures higher in the chart cannot be used unless procedures lower in the chart have been tried or would be too risky or dangerous to try. Also, the techniques that will be placed in a tier will probably be new techniques using newly developed technologies, not well-established police techniques.

Another possible objection is that requiring the police to exhaust second-best possibilities doesn't allow for flexible, rapid police response. Again, I can't agree. First, the techniques listed in the chart above tend not to be techniques used on the spur of the moment. These are deliberative steps used in methodical investigations, not quick-response tactics. In fact, nearly every procedure listed in the chart above (save data mining) requires judicial authorization today,

⁶¹ [Cites from Slobogin.]

DRAFT VERSION: PLEASE DO NOT CITE

which suggests that the police don't do these things on the spur of the moment under current law. Second, many "traditional" techniques and procedures will probably never be assigned a tier. What the police know from past training will probably be available to them in any order. Third, tiered necessity can be coupled with emergency exceptions, which allow the police to take a tiered step out of sequence, in cases of danger to life or limb.⁶²

2. A Better Remedy

The main problem with the Stored Communications Act is that it doesn't provide adequate remedies for aggrieved parties.⁶³ It provides victims of violations with limited civil remedies against the ISP⁶⁴ and even more limited remedies against the law enforcement agents.⁶⁵ Suppression is not available.⁶⁶ Criminal defendants, therefore, have no reason to challenge suspected violations, and the case law remains woefully underdeveloped.⁶⁷

One suggestion for the SCA and for privacy-regulating statutes generally is to have violations reflected in the recommended sentence in the sentencing guidelines. Post-*Booker* and *Rita*, the guidelines are merely discretionary but presumptively reasonable. The guidelines could be amended to provide that convictions that result from a violation of the SCA lead to a downward departure of two or three levels in the recommended sentence.

This would have several salutary effects. First, defendants would have an incentive to litigate perceived violations of the SCA, and judges would have the opportunity to interpret the law and give Congress better feedback on the law in operation. Second, this litigation would not occur at the guilt-or-innocence phase, but would instead happen during the less-charged sentencing phase. In fact, it might even encourage plea bargaining where guilt is admitted but the right to challenge the privacy violation reserved.

⁶² [SCA 2702 exceptions]

⁶³ [Kerr on suppression]

⁶⁴ 18 U.S.C. § 2707(a) (providing a civil cause of action for violations against any "person or entity, other than the United States).

⁶⁵ 18 U.S.C. § 2707(d) (providing a very weak suggestion of administrative discipline against government employees who violate the law).

⁶⁶ 18 U.S.C. § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.").

⁶⁷ [Kerr.]

DRAFT VERSION: PLEASE DO NOT CITE

Third, the police will object less to the proposal than they have to past suppression proposals, because their violations of these often-confusing laws will not result in lost convictions, but instead in lowered sentences. At the same time, the prospect of lost convictions will probably be enough to place more compliance-pressure on the police. Even if it doesn't standing alone, the fact that more of their actions will be scrutinized and litigated, and the fact that adverse rulings can be used for follow-on civil lawsuits will probably be a strong motivating factor.

3. A Return to Old-Style Minimization

The police should not be allowed to minimize wiretapped, electronic communications after-the-fact. Minimization itself embodies the balance between security and privacy. We force the police to throw away potential evidence, because we won't let them tread on too much privacy to make their case. After the fact keyword searching loses sight of this feature, allowing the police to try to prove how clever they are at decoding and deciphering the keywords used by their quarry.

Conclusion

This is the first piece of a larger project. The overarching idea is that tools directly drive the privacy/security debate, by providing solutions that act either in a zero-sum, winner-take-all way, or that force us to think about trade-offs and encourage us to balance. This article has focused entirely on legal tools, law enforcement exceptions that work better than mere justification standards to those ends.

The next step in the project is to focus on non-legal tools, and particularly for the information privacy debate, on technological tools. The debate about how much privacy-enhancing technology we should have mirrors the debate criticized in this article. It is zero-sum and extreme, with one side calling for perfect, virtually uncrackable encryption for all, and the other side—sometimes-publicly, usually-secretly—hoping for a ban on such technology.

There are other tools that more comfortably sit between these extremes, that like tiered necessity, make it hard but possible for the police to access private communications. These tools, I will argue later, are the tools we should desire for many reasons, including the counter-

DRAFT VERSION: PLEASE DO NOT CITE

intuitive reason that we have never had perfect anonymity in the real world, and that we should not desire it online.