
NEW YORK UNIVERSITY
JOURNAL OF LAW & LIBERTY

SHRINKING THE INTERNET

Philip A. Wells*

INTRODUCTION

The Internet presents unique policing challenges, but these challenges share striking similarities with those in densely populated cities. Both environments are staggering in scope and size, regularly exposing citizens to strangers, unconventional norms, and deviant behavior.[1] And despite their frenetic environments, both foster feelings of remoteness and anonymity.[2] This sentiment, in tandem with the scale of both the Internet and large cities, inhibits the growth of social norms: informal interactions that help communities self-police and shame potential criminals.[3]

---

* Philip A. Wells is 2009 graduate of the New York University School of Law and can be reached via e-mail at philip.a.wells@gmail.com. He hopes you don't use this contact information in furtherance of a cybercrime.

[1] *Compare* LYN H. LOFLAND, A WORLD OF STRANGERS: ORDER AND ACTION IN URBAN PUBLIC SPACE, at ix–x (1973) ("To experience the city is, among many other things, to experience anonymity. To cope with the city is, among many other things, to cope with strangers.") *with* Mattathias Schwartz, *Malwebolence*, N.Y. TIMES, Aug. 3, 2008, § MM (Magazine), at MM24 (exploring the malicious interaction between trolls and strangers on the internet).

[2] *Compare* LOFLAND, *supra* note 1, at 10 ("This is hardly an earth-shaking observation. Everyone knows that cities are 'anonymous' sorts of places.") *with* George F. du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 191, 192 (2001) ("Anonymity . . . is easier to attain than ever before due to the recent emergence of cyberspace.").

[3] *See* Lior Jacob Strahilevitz, *Social Norms From Close-Knit Groups to Loose-Knit Groups*, 70 U. CHI. L. REV. 359, 362 (2003) ("Cooperation on a peer-to-peer [internet]

Part I will show how these social norms exert an enormous influence over law-abiding behavior. Wherever social norms struggle to spontaneously grow, policymakers lose a critical crime-fighting device. On the Internet, this loss creates a strong temptation to fill the enforcement vacuum with enhanced government intervention.[4] This temptation, however, is misguided. In the city, such techniques have yielded controversial results, as Part II will illustrate.[5] And on the Internet, where such techniques are being proposed, invasive law enforcement tactics will prove costly, oppressive, and foster a dangerous disrespect for privacy in the digital age.[6]

This note proposes a recalibration of Internet policing to incorporate lessons learned from the urban environment. Part III will show how this is possible, by describing the critical similarities between the

---

network, subway, or freeway cannot result from signaling or esteem-seeking, the two most persuasive explanations for how social norms arise in close-knit groups."); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1008 (2001) ("Social norms cannot operate as effectively to prevent crime on the net because its users are not necessarily constrained by the values of realspace."); April Mara Major, *Norm Origin and Development in Cyberspace: Models of* Cybernorm *Evolution*, 78 WASH. U. L.Q. 59, 84 (2000) ("[T]he anonymity afforded by digital communication gives individual users the freedom to ignore or modify existing social norms that they find unsatisfactory.").

[4] Katyal, *supra* note 3, at 1008 ("Each new major cybercrime leads law enforcement to push for changes to the technical infrastructure to create better monitoring and tracing.").

[5] Bernard E. Harcourt & Jens Ludwig, *Broken Windows: New Evidence from New York City and a Five-City Social Experiment*, 73 U. CHI. L. REV. 271, 314–16 (2006) (concluding, after empirical analysis, no evidence that increased police attention to misdemeanor violations reduces crime); Bernard E. Harcourt, *Reflecting on the Subject: A Critique of the Social Influence Conception of Deterrence, the Broken Windows Theory, and Order-Maintenance Policing New York Style*, 97 MICH L. REV. 291, 331–32, 386– 89 (1998) [hereinafter Harcourt, *Reflecting*] (stating that the New York "broken windows" policy did not play a significant role in reducing crime rates).

[6] *See* Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS L. REV. 267, 281–84 (2002) (discussing the complexities involved in determining jurisdiction over computer crime internationally); Ann E. Carlson, *Recycling Norms*, 89 CAL. L. REV. 1231, 1235 (2001) ("When numerous people must act to solve a collective problem and lack the economic incentive to do so, traditional government regulation . . . may be infeasible, ineffectual, or politically difficult. The costs of monitoring and enforcement can be prohibitively expensive or may raise privacy concerns."). For ways in which draconian tactics may undermine legal legitimacy, see *infra* Part IV.

Internet and the city. Through this analogy, Internet policymakers can learn important lessons from past city policing experiments, and perhaps more importantly, avoid historical urban blunders.

As Part IV will illustrate, Internet policing is currently at a unique crossroads between harnessing urban lessons and repeating them. At this critical moment, Internet policymakers should learn from urban policing and encourage more intimate social norms on websites.[7] In order to act most efficiently, Internet policymakers should focus on the enforcement mechanisms in Part V—user registration, structural transparency, opt-in disclosures, and visitor-to-visitor communication—that can transform sprawling, urban-like websites into Internet "villages," capable of robust social norms. These techniques, which are already available to website administrators, would effectively shrink the Internet, normalizing online interaction and discouraging antisocial behavior.

Law enforcement officials and policymakers should pay heed to this self-policing activity and abandon an invasive one-size-fits-all approach to the Internet. Through these devices, website administrators would enhance the policing process by allowing Internet users to police themselves. By enabling Internet users to become an empowered, grassroots group of digital detectives in their online communities, the Internet can become a place to participate in the law enforcement process instead of a place to avoid it. Such enhanced user participation would maximize the effectiveness of limited law enforcement resources and reduce the illusory trade-off between freedom and security on the Internet.

PART I: AN EXPLANATION OF SOCIAL NORMS

A. Social norms are extralegal constraints that suppress individuals from undesirable impulses when they feel—or have been conditioned to feel—the scrutiny of their peers.

---

[7] The concept of calibrating government regulation to growing social norms on the internet is not new. *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 99 (1999). But while Lessig focuses on the regulation of software and browser "code" on each computer, this note focuses on the websites existing on the internet itself.

"But child, what would people think?" Disapproving family members and friends are perhaps the best illustration of social norms. By wielding shame, guilt, and a watchful eye, loved ones have an arsenal with which they can influence each other's behavior. And when these weapons are effectively employed in a community at-large, they are called social norms.

Technically, legal scholars define social norms as extralegal constraints that compel individuals, both consciously and subconsciously, to take certain action when defiance would "subject them to sanctions from others," make them feel guilty, or both.[8] Fearing social retribution, individuals tend to restrict the ambit of their action—even in the absence of law enforcement—when they feel the scrutiny of their peers. In this way, social norms sustain inertia capable of inhibiting antisocial and criminal behavior.

B. Social norms provide the backdrop for legal action.

Since social norms are capable of developing organically, without the use of arduous legislation and costly policing, they are a low-cost means of influencing behavior.[9] Due to this advantage, law-and-norms literature has proliferated: over the past decade, scholars have used social norms to explain a wide range of human behavior that includes voting,[10] recycling,[11] pirating music,[12] and even sumo wrestling.[13]

This wide applicability makes social norms a powerful lens through which legal scholars can analyze legal problems. Specifically, "[n]orms matter to legal analysis because (1) sometimes

---

[8] Carlson, *supra* note 6, at 1238. *See also* Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 341 (1997).

[9] *See, e.g.*, Todd J. Zywicki, *An Economic Analysis of the Consumer Bankruptcy Crisis*, 99 NW. U. L. REV. 1463, 1532 (2005) ("Social norms are valuable as a mechanism for social control because they are generally a low-cost mechanism for promoting exchange that substitutes for more costly financial institutions such as security and increased monitoring by creditors.").

[10] *See* Richard L. Hasen, *Voting Without Law?*, 144 U. PA. L. REV. 2135, 2136, 2138–64 (1996).

[11] *See* Carlson, *supra* note 6.

[12] *See* Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505 (2003).

[13] *See* Mark D. West, *Legal Rules and Social Norms in Japan's Secret World of Sumo*, 26 J. LEGAL STUD. 165 (1997).

norms control individual behavior to the exclusion of law, (2) sometimes norms and law together influence behavior, and (3) sometimes norms and law influence each other."[14] Without an understanding of social norms, otherwise well-intentioned law enforcement may prove costly, impotent, or even counterproductive.[15] But with a better understanding of social norm dynamics, legislation and law enforcement can become less costly, more feasible, and more effective.

C. Traditionally, social norms have only been studied in "close-knit" contexts.

Social norms scholarship famously began in a distinctly non-urban, non-Internet context. In *Order Without Laws*, Robert Ellickson launched the social norms movement by cataloging the interplay between cattle ranchers in an isolated California county.[16] According to Ellickson, the Shasta County ranchers resolved cattle-trespass disputes through informal rules, and legal rules "hardly ever influence[d]" the resolution.[17] Whenever a neglectful rancher failed to supervise his cattle and allowed strays to damage a neighbor's property, the victim rarely went to court—or even an attorney—to resolve the issue.[18] In fact, the community held official legal action in such low regard that if a rancher *did* hire an attorney to resolve a dispute, he or she was considered a community outsider—an "odd duck."[19]

Instead, the ranchers resorted to negative gossip.[20] The importance of personal reputation and generations-long "family names"

---

[14] McAdams, *supra* note 8, at 339.

[15] Carlson, *supra* note 6, at 1235 ("The enthusiasm for social norms management as a solution to large-number, small-payoff collective action problems may stem from the fact that other regulatory methods are often unsatisfactory. When numerous people must act to solve a collective problem and lack the economic incentive to do so, traditional government regulation . . . may be infeasible, ineffectual, or politically difficult. The costs of monitoring and enforcement can be prohibitively expensive or may raise privacy concerns.").

[16] *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).

[17] *Id.* at 40.

[18] *Id.* at 60.

[19] *Id.* at 64.

[20] *Id.* at 57.

in Shasta Country made social control powerful enough to make neglectful ranchers apologize, resolve the issue, and compensate the victim outside of the courtroom.[21] These social norms were effective beyond the shadow of the law, Ellickson posited, because these ranchers felt the social inertia of "neighborliness," knew each other personally, and interacted with one another on a regular basis.[22]

In short, the ranchers were a "close-knit" community, and this is what made the gossip so powerfully potent. In technical terms, Ellickson described the ranchers as a "close-knit group" because both the informal social control (e.g., negative gossip) and the information necessary for such control (knowledge of others' behavior) were broadly available to each and every group member.[23] Ellickson argued that Shasta County's social norms grew from this intimacy, or close-knittedness, and that if the ranchers had been structurally impaired from knowing "how particular [ranchers] acted in the past in particular social interactions," it is "still anyone's guess" whether social norms would have developed at all.[24] Outside of close-knit groups, Ellickson was "agnostic about whether social norms [could] emerge" at all.[25]

D. This note joins mounting literature that extends social norms beyond the "close-knit" context.

This note picks up where Ellickson left off. Since *Order Without Laws*, legal scholars have begun examining how social norms might arise outside of "close-knit" contexts, where individuals are more anonymous and interact less regularly.[26] Unlike close-knit groups, "[t]hese loose-knit groups are typically composed of members who do not expect to be repeat players or who are unable to gather accurate information about another member's reputation even if repeat-player interactions do occur."[27] In the following sections, this note will show how the city and the Internet are loose-knit groups,

---

[21] *See id.* at 53–57.

[22] *Id.* at 53–64.

[23] *Id.* at 177–78.

[24] *Id.* at 181.

[25] *Id.* at 177.

[26] Strahilevitz, *supra* note 3, at 359. *See, e.g.*, Carlson, *supra* note 6; Major, *supra* note 3.

[27] Strahilevitz, *supra* note 3, at 360.

where the lack of repeat interaction renders gossip and social embarrassment ineffective. While legal scholars have already begun considering social norms consequences for "loose-knit group" applications that the use Internet (e.g., file-sharing computer software),[28] none have systematically explored the potential for social norm growth *across different* websites on the Internet.[29] Until now, none have tried to dissemble the Internet at-large into discrete parts capable of intimate social norm growth; none have tried to "shrink" the Internet from a sprawling loose-knit group into a series of close-knit communities. That is the objective of this note, in large part, through an analogy of another famously non-close-knit context, the city.[30]

PART II: SOCIAL NORMS IN CITIES

Well it's hard to live, it's hard to live in the city
Yes it's hard to live, so hard to live in the city

I've been following you for blocks and I wish you would stop and tell me your name
But I couldn't understand what you told me as you ran away

So just lay your head down low,
Don't let anybody know
That it's hard to live, it's hard to live in the city

---

[28] Strahilevitz, *supra* note 12, at 547; Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. REV. 457, 469–74 (2001); Major, *supra* note 3; Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT. L. REV. 1257 (1998). Only Strahilevitz refers to loose-knit groups as such.

[29] *See, e.g.*, Strahilevitz, *supra* note 3 at 361 ("In the twelve years since the publication of *Order without Law*, no legal scholar has looked at loose-knit groups systematically.").

[30] This note refers to the "city" in terms of its public spaces: streets, sidewalks, restaurants and public squares that are generally available to citizens—and where socialization normally occurs. The limits of this term will continue analogously on the Internet: this note's argument addresses only "publicly-available" websites. Perhaps counter-intuitively, this limit *strengthens* this note's insistence that governments should avoid a "one-size-fits-all" approach to policing cyberspace and should carefully calibrate policing depending on the social norms residing in each website community, private or not.

Yes it's hard to live, it's hard to live in the city[31]

Although capable of enhancing law-abiding behavior, social norms are often thwarted in the dense urban environments. As discussed below, the existence of strangers and anonymity in crowded cities cripple the ability for social norms to constrain criminal behavior. Accordingly, city governments have deployed a variety of experimental—and controversial—legal responses to reduce criminality. These experiments have produced important policing lessons that scholars can extend to the Internet and other loose-knit contexts. In particular, these lessons illustrate the costs of invasive policing in loose-knit communities and emphasize the problems to avoid when addressing crime on the Internet.

A. Anonymity devastates the development of social norms.

1. POPULATION ENORMITY IN CITIES ALLOWS ITS INHABITANTS TO LEAD ANONYMOUS LIVES.

In various city public spaces, including streets, sidewalks, and subway cars, high levels of population size and density create a "peculiar social situation": city-inhabitants become strangers to one another.[32] Since there are so many city-inhabitants in any given location at any given moment, it is impossible for inhabitants to personally know the vast majority of people they come in contact with. "Each knows of the aggregate existence of all these others, of course, but [any one inhabitant] does not know of [others'] individual existence: he does not know their names or their personal histories or their hopes or preferences or fears."[33] Regular collision with complete strangers—and the expectation of such collision—allows city-inhabitants to lead an anonymous public existence.[34]

---

[31] ALBERT HAMMOND, JR., *Hard to Live in the City*, *on* YOURS TO KEEP (New Line Records 2007).

[32] LOFLAND, *supra* note 1, at 3.

[33] *Id.*

[34] *See id.* at ix.

2. ANONYMITY IMPAIRS SOCIAL NORMS BECAUSE DEVIANTS ARE LESS LIKELY TO GET CAUGHT.

Anonymity severely debilitates social norms because it impairs deviance detection; it eliminates the risk that city-inhabitants will be "caught" and punished by their social circles if they commit a wrong.[35] If, for example, a stranger were to steal a bicycle from a city sidewalk, with whom could the victim reasonably gossip in order to make the stranger feel guilty for his actions? In Ellickson's Shasta County, ranchers would turn to their neighbors and friends: each member of the community interacted with the other members so regularly that ranchers could gossip with almost anyone to punish a thief.[36] But urban communities lack such social cohesion. Even if the city victim spoke about the incident to every single person she knew, there is little reason to believe that this gossip would even reach the stranger, much less damage his reputation or make him feel guilty.

In this way, anonymity—and the low degree of social cohesion it signifies—impairs neighbors from taking active responsibility for order in the community. This phenomenon is perhaps best illustrated in terms of game theory: since the city-victim and the stranger are non-repeat players engaged in single-shot play, there is little social cost that the victim (or her friends) can exact on the stranger. Outside of very serendipitous circumstances, the victim will not know the stranger's name, address, or the people with whom the stranger values his reputation.[37] Without this critical information, city-inhabitants cannot know where or how to feasibly enforce social norms.[38] This makes city public spaces a quintessentially loose-knit: the informal

---

[35] Patrick J. Keenan, *Do Norms Still Matter? The Corrosive Effects of Globalization on the Vitality of Norms*, 41 VAND. J. TRANSNAT'L L. 327, 369 (2008) ("If people are certain that there is no chance that their behavior will be discovered, then rewards and sanctions, apart from those that are purely internal, are irrelevant.").

[36] *See* Ellickson, *supra* note 16, at 55–64.

[37] Keenan, *supra* note 35, at 369 ("Put another way, members of the community must be part of the same reputation market. The person whose behavior is at issue must be susceptible to the punishments, or must desire the rewards available to those who observe her behavior and would enforce the norm.").

[38] *See id.* ("If people are certain that there is no chance that their behavior will be discovered, then rewards and sanctions, apart from those that are purely internal, are irrelevant. Information is thus essential to the emergence and vitality of norms.").

social control (e.g., negative gossip) and the information necessary for such control (knowledge of others' behavior) are not broadly available to all the individual group members.[39] In fact, they are hardly available to anyone at all.[40]

B. Fear of a social norm vacuum created a misguided legal response: the broken windows policy

As illustrated above, information failure—a product of anonymity—cripples the ability of social norms to constrain criminal behavior. It strips neighbors of their social tools and impairs them from acting as informal watchmen for the community. In response to this problem, legal scholars initially turned to the formal watchmen of the community—the police—to fill the vacuum in enforcement.[41]

Led by George Kelling, these legal scholars argued for a "broken windows" policy to "take back the streets" and reestablish social norms, which they called "a modicum of civility and safety" for urban citizens.[42] Kelling and others recommended the use of aggressive police tactics to eliminate small signs of disorder in city public spaces, like a broken window, that would have otherwise been deterred by social norms. If left unattended, they warned, these low-level signs of disorder would fester and eventually erupt in the form of violent crime. According to the theory, this eruption occurs when cities tolerate minor signs of disorder, such as loitering, prostitution, and pan-handling,

---

[39] *Id.* at 377–78.

[40] At this point it is important to recognize that city public spaces are not always lawless, and social norms are not the only mechanisms that influence law-abiding behavior. A dearth of robust social norms does not create lawlessness; it merely leaves areas more exposed to it.

[41] *See* Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349, 352 (1997) ("[I]t might make sense for the government to assume a greater share of the burden in preventing crime than the standard view suggests is optimal."). *See generally* Reed Collins, *Strolling While Poor: How Broken-Windows Policing Created a New Crime in Baltimore*, 14 GEO. J. ON POVERTY L. & POL'Y 419, 422 (2007) ("The broken windows theory is by now a familiar justification for aggressive policing strategies that include custodial arrests for such minor 'quality-of-life' crimes as public urination, public drinking, and disturbing the peace.").

[42] GEORGE L. KELLING & CATHERINE COLES, FIXING BROKEN WINDOWS 108 (1996), *based on* George L. Kelling & James Q. Wilson, *Broken Windows: The Police and Neighborhood Safety*, ATLANTIC MONTHLY, Mar. 1982, at 29.

because neglect in enforcement sends a "signal to potential criminals that delinquent behavior will not be reported or controlled—that no one is in charge."[43] This signal then results in a vicious cycle: criminally-inclined individuals, unchecked by social norms, are emboldened by the neglect and engage in increased criminal behavior, which prompts law-abiding individuals to flee the blighted area. By staying indoors or leaving the community entirely, these law-abiding individuals effectively abandon the public spaces where they might ordinarily exercise social norms. As these informal checks on undesirable behavior continually deteriorate, this abandonment only encourages criminals to commit more crime. In this way, apparent disorder—the broken window—begets *actual* disorder, and "invites other broken windows," which "progressively break down community standards and leave the community vulnerable to crime."[44]

Fearing this vicious cycle, cities nationwide quickly signed onto the broken windows policy. With invasive policing and harsher penalties, Boston began aggressively enforcing "quality of life" offenses like turnstile jumping in its underground "T" subway system.[45] Chicago implemented a loitering ordinance and enforced it so vigorously that between 1993 and 1995 the city had arrested over 42,000 individuals for the offense.[46] Perhaps most famously, Rudolph Giuliani made broken windows the cornerstone of his campaign for New York City mayor in 1992 and even quoted George Kelling during his speeches.[47]

---

[43] BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING 24 (2001) [hereinafter HARCOURT, ILLUSION].

[44] *Id.*

[45] Daniel Brook, *The Cracks in 'Broken Windows,'* BOSTON GLOBE, Feb. 19, 2006.

[46] *See* City of Chicago v. Morales, 527 U.S. 41, 49 (1999).

[47] Brook, *supra* note 45 ("In a 1992 speech kicking off his campaign, Giuliani quoted from Kelling and Wilson, adding his own prosecutorial gloss. Aggressive panhandlers and squeegee men were not nuisances, Giuliani said, they were criminals.").

It was an age of bellicose—and constitutionally questionable[48]—police action against misdemeanor offenders. In New York alone, misdemeanor arrests "soared by 50%, from 133,466 in 1993 to 205,277 in 1996."[49] And according to New York City crime statistics, it was just the right medicine: between 1994 and 1996, murders fell by 39%, auto-theft by 35%, robberies by a third and burglaries by a quarter.[50] Overall, crime in New York was down 50% from 1990, outpacing the national average.[51]

City officials and broken windows scholars declared victory.[52] In January 1996, Time magazine called it a "miracle," "New York's magic," and featured New York Police Commissioner William Bratton on the cover.[53] The Los Angeles Times called it the "Holy Grail" of the 1990s.[54] Praise for aggressive policing was so unanimous that in 1998, a leading skeptic lamented that it was "practically impossible to find a single scholarly article that takes issue with the [broken windows] quality-of-life initiative. It stands, in essence, uncontested—even in the legal academy."[55]

Since 1998, however, legal scholars have retreated from widespread adulation of the broken windows policy.[56] In various works,

---

[48] *See* City of Chicago v. Morales, 527 U.S. 41, 41 (1999) (overruling the Chicago anti-loitering ordinance as unconstitutionally vague); *see also* Andy Newman, *Ruling in Street Crime Unit Case Could Expand List of Plaintiffs*, N.Y. TIMES, Jan. 26, 2001, at B6 ("A 1999 review by the state attorney general's office of thousands of stop-and-frisk reports by the [New York City] Street Crime Unit found that there was no reasonable cause for 23 percent of the stops . . . . [and] [i]n October, the federal Justice Department determined that the unit's officers had routinely engaged in racial profiling."); Ford Fessenden & David Rohde, *Dismissed Before Reaching Court, Flawed Arrests Rise in New York*, N.Y. TIMES, Aug. 23, 1999, at A1.

[49] Collins, *supra* note 41, at 428 (citing HARCOURT, ILLUSION, *supra* note 43, at 101).

[50] Eric Pooley & Elaine Rivera, *One Good Apple*, TIME, Jan. 15, 1996, at 54; Harcourt, *Reflecting*, *supra* note 5, at 331–32 (1998) [hereinafter Harcourt, *Reflecting*].

[51] *Id.* Harcourt, *Reflecting*, *supra* note 5, at 331–32.

[52] *Id.* (citing Kahan, *supra* note 41).

[53] *Id.*

[54] *Id.* at 292 (citing Robert Jones, *The Puzzle Waiting for the New Chief*, L.A. TIMES, Aug. 10, 1997, at B1).

[55] *Id.* at 293. *See also* HARCOURT, ILLUSION, *supra* note 43, at 101 ("The brute fact is that misdemeanor arrests in New York City increased dramatically once Mayor Giuliani took office.").

[56] *See* Collins, *supra* note 41, at 427 ("Applying theory to practice, the success of broken-windows policing in American cities is still difficult to determine. While some commentators credit broken-windows policing for an impressive decline in

Bernard Harcourt marshaled enormous amounts of empirical data to show that Giuliani's police tactics did not play a statistically significant role in reducing New York's crime rates.[57] Instead, Harcourt emphasized that (1) new crime-fighting technology like the "Compstat" computer system made existing police efforts more efficient,[58] (2) dramatic increases in the size of the police force gave the city more resources to combat crime,[59] and (3) favorable shifts in economic conditions, city demographics, and drug-demand in the 1990s may have destabilized urban violence.[60]

Similarly, Robert Sampson and Stephen Raudenbush analyzed Chicago crime figures and reported that (1) social norms (which they called "collective efficacy") more closely related to crime than the physical symbols of disorder that police were targeting and (2) these social norms were not statistically related to the targeted disorder.[61]

C. Broken windows policy led to high social costs and negative consequences.

By 2007, scholars admitted that the evidence behind the broken windows police tactics "remains, at best, mixed,"[62] "unproven,"[63] and "controversial."[64] But in addition to questioning its past effectiveness, legal scholars have now begun questioning the future tenability of broken windows policing. Today, scholars note that the broken windows policies in New York and Chicago had many unintended racial

---

crime rates during the 1990s, others see oppression of African Americans and the poor and attribute gains in the fight against crime to larger social forces.").

[57] Harcourt & Ludwig, *supra* note 5, at 314–16 (concluding, after empirical analysis, that increased police attention to misdemeanor violations does not reduce crime); Harcourt, *Reflecting*, *supra* note 48, at 386–89 (stating that the New York "broken windows" policy did not play a significant role in reducing crime rates).

[58] HARCOURT, ILLUSION, *supra* note 43 at 98.

[59] *Id.* at 94–96.

[60] *See id.* at 97–100.

[61] Collins, *supra* note 41 at 466–67 (citing Robert J. Sampson & Stephen W. Raudenbush, *Systematic Social Observation of Public Spaces: A New Look at Disorder in Urban Neighborhoods*, 105 AM. J. SOC. 603, 622–30 (1999)).

[62] Harcourt & Ludwig, *supra* note 5, at 272.

[63] Collins, *supra* note 41, at 421.

[64] Eduardo Moisés Peñalver & Sonia K. Katyal, *Property Outlaws*, 155 U. PA. L. REV. 1095, 1150 n.237 (2007).

and socio-economic consequences, threatening the legitimacy of both the broken windows policy and the police forces that implemented it.

1. BROKEN WINDOWS POLICY RESULTED IN LEGALLY QUESTIONABLE POLICING TACTICS.

In theory, broken windows was simply an effort to constitutionally increase police presence on city streets. But in practice, aggressive policing often operated at the edges of constitutionality. In 1999, the Supreme Court struck down a Chicago broken windows ordinance forbidding individuals from remaining "in any one place with no apparent purpose"[65] after police had arrested 42,000 for the crime.[66] That same year, the New York state attorney general's office reported that nearly one-fourth of the "thousands of stop-and-frisk[s]" by New York City police officers lacked reasonable cause and were therefore illegal.[67] Also in 1999, the *New York Times* reported that New York City police falsely arrested fifty people *per day*, who were "processed through the [New York] booking system and released because prosecutors reject[ed] the charges against them, often after they [had] spent hours or overnight in packed holding cells."[68]

For many citizens, broken windows meant daily violations of the Constitution. One such false-arrest was documented in a 1999 *New York Times* article:

> 'It was horrible,' said Oona Chatterjee, a New York University Law School graduate who was arrested on a fall day last year. . . . Ms. Chatterjee, who runs a neighborhood legal clinic in Bushwick, spent 15 hours in a Brooklyn precinct house handcuffed to the bars of a holding cell. Trying to intervene for residents of an apartment building who were watching an altercation between the police and a neighborhood resident, she was arrested and taken to the 83d Precinct station.

---

[65] City of Chicago v. Morales, 527 U.S. 41, 47 n.2 (1999).
[66] *Id*. at 49.
[67] Newman, *supra* note 48.
[68] Fessenden & Rohde, *supra* note 48.

> She was released, with no charges filed, after 22 hours in custody. The city paid a $45,000 settlement to Ms. Chatterjee last month without contesting her false-arrest lawsuit.[69]

2. AN UNEVEN APPLICATION OF THESE CONSTITUTIONALLY QUESTIONABLE POLICE TACTICS FORCED SOME COMMUNITIES TO BEAR THE BRUNT OF BROKEN WINDOW MORE THAN OTHERS.

These false-arrests and questionable stop-and-frisks would be troubling anywhere; such behavior makes the citizenry lose faith in the competence and intentions of its police force. But it had a particularly devastating effect in the context of the broken windows policy, where ethnic minorities and the poor felt the brunt of such tactics.[70]

This unequal application stems largely from the theory itself. Broken windows is a policy that focuses on appearance; it has "little to do with fixing broken windows and much more to do with arresting window breakers—or persons who look like they might break windows."[71] As a result, broken windows policing concentrates on highly visible, street-level crimes.

Due to the fact that "high-density minority neighborhoods . . . tend to have a more active street life than more affluent areas," broken windows policing is more likely to take place in these areas.[72] As a result, disadvantaged areas disproportionately shouldered the devastating side effects of the broken windows policy: "in the two police precincts that make up Washington Heights, Inwood and northern Harlem," traditional minority neighborhoods in New York City, "prosecutors threw out 120 of the 2,035 arrests [in 1999]—a rate, 5.9 percent, that is about twice as high as in the rest of Manhattan during that period."[73] As one legal scholar decried, broken windows made

---

[69] *Id.*

[70] *See* Collins, *supra* note 41, at 425–27; Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 331, 333 n.1 (1998) (quoting Ann Belser, *Suspect Black Men Are Subject to Closer Scrutiny from Patrolling Police, and the Result Is Often More Fear, Antagonism Between Them*, PITTSBURGH POST-GAZETTE, May 5, 1996, at A15).

[71] Harcourt, *Reflecting*, supra note 5, at 342.

[72] Jerome Skolnick, *Good Cop*, 4 DEMOCRACY: J. IDEAS 92, 97 (2007), *available at* http://www.democracyjournal.org/pdf/4/092-099.skolnick.FINAL.pdf. .

[73] Newman, *supra* note 48.

"strolling while poor" in cities a crime.[74] Despite any good intentions, broken windows was inadvertently stoking racial and class-based animus.

Instead of preventing the broken windows in the community, broken windows policies "devastate[d] the communities [they were] supposed to protect" by disproportionately affecting minority neighborhoods.[75] At an individual level, members of socially-disadvantaged communities were now "more likely to have a criminal record preventing them from obtaining well-paying jobs and livable housing."[76] At the community level, these neighborhoods—targeted based on the appearance and without apparent regard for an individual's innocence or guilt—diminished critical civilian support for their police forces and the rule of law.[77] Each successive unconstitutional stop-and-frisk prompted targeted minorities to perceive city governments as illegitimately classist and racist,[78] and this sentiment only increased with the warrantless arrests,[79] unconstitutional searches,[80] and questionable ordinances[81] that too-often accompanied the broken windows policy.

The combination of these two problems—tendencies toward illegal policing and uneven application—made New York a policing powder keg by the new millennium. This powder keg erupted on February 1999 when Amadou Diallo, "an unarmed West African

---

[74] *See generally* Collins, *supra* note 41 (discussing Baltimore's broken windows policies, specifically modeled after New York).

[75] Eric J. Miller, *Role-Based Policing: Restraining Police Conduct "Outside the Legitimate Investigative Sphere,"* 94 CAL. L. REV. 617, 631 (2006).

[76] Collins, *supra* note 41, at 426.

[77] Miller, *supra* note 75, at 623 ("The style and consequences of policing often lead to a public perception of institutional illegitimacy, where the minority, urban community internalizes the style and consequences of policing as race-based and racist.").

[78] Collins, *supra* note 41, at 426–37 (citing DAVID COLE, NO EQUAL JUSTICE 46 (1999)); Jeffrey Fagan & Garth Davies, *Street Stops and Broken Windows:* Terry*, Race, and Disorder in New York City*, 28 FORDHAM URB. L.J. 457, 462 ("The fact that its principle tactic was an aggressive form of stop and frisk policing involving intrusive *Terry* searches, and that at least two deaths of unarmed citizens of African descent were linked to OMP, further intensified perceptions of racial animus.").

[79] Fessenden & Rohde, *supra* note 48.

[80] Newman, *supra* note 48.

[81] *See* City of Chicago v. Morales, 527 U.S. 41 (1999) (overruling the Chicago anti-loitering ordinance as unconstitutionally vague).

immigrant with no criminal record" was gunned down by police with a flurry of forty-one bullets.[82] According to police sources, Mr. Diallo attracted police officers' attention because he was loitering and "acting suspicious" near his Bronx home.[83] Although the facts surrounding this early morning shooting remained controversial, the officers involved said "they had thought he had a gun. It turned out to be a wallet."[84] Broken windows policy had claimed a person's life.

The ensuing days—and eventual acquittal of the police officers—rocked the city with outrage and violent protests. Amadou Diallo became "shorthand for excessive police force against minorities,"[85] and even former Police Commissioner William Bratton, the architect of broken windows policing in New York City, began criticizing aggressive stop-and-frisks in a *New York Times* editorial.[86] According to Bratton, broken windows was an excellent tactic during crime waves, but when crime declined, minority populations "had every right to expect that one of the benefits of living in a safer city would be less police intrusion into their everyday lives."[87] In ten short years, broken windows had gone from being the "Holy Grail"[88] to a short-term tactic of last resort.

3. BROKEN WINDOWS THREATENS THE REPUTATION AND LEGITIMACY OF CITY GOVERNMENTS.

Once considered the panacea of crime-fighting, broken windows techniques are now the problem. The history of bellicose policing now poses a "legitimacy crisis" to police forces in minority neighborhoods, "resulting from justified public perceptions of a disjunction between the promise of equal treatment by the

---

[82] Michael Cooper, *Officers in Bronx Fire 41 Shots, and an Unarmed Man Is Killed*, N.Y. TIMES, Feb. 5, 1999, at A1.

[83] *Id.*

[84] Jane Fritsch, *4 Officers in Diallo Shooting Are Acquitted of All Charges*, N.Y. TIMES, Feb. 26, 2000, at A1.

[85] Manny Fernandez, *In Bell Case, Black New Yorkers See Nuances That Temper Rage*, N.Y. TIMES, Apr. 27, 2008, at A1.

[86] Skolnick, *supra* note 72, at 98.

[87] *Id.*

[88] Robert Jones, *The Puzzle Waiting for the New Chief*, L.A. TIMES, Aug. 10, 1997, at B1 (quoted in Collins, *supra* note 41, at 421).

criminal justice system and the reality of certain laws and policing practices."[89] As a result of this resentment, tension develops between law-abiding citizens and the police—the institutional representation of law on streets. Social norms are pitted against legal norms, symbols of law are pitted against notions of justice, and the police are isolated from the very communities that need policing most.

This is no small cost, and cities cannot afford it. As Jeffery Fagan notes, "[p]eople who view the law as illegitimate are less likely to obey it, and people who view police officers and judges as lacking in legitimacy are less likely to follow their directives."[90] This is particularly toxic in cities because police need citizen cooperation to fight crime, regardless of the tactics they employ. Citizens not only help police their neighborhoods informally, but also report crime, allow themselves to be interviewed by police after crimes have been committed, and act as jurors and witnesses before the court once a suspect has been identified. When citizen cooperation breaks down, the police become an impotent force: it is both more cumbersome to prevent crime and more difficult to solve crimes and convict criminals. This is the true harm of invasive police techniques. In post-broken windows cities, police both lose the social norms arsenal available in close-knit communities and gain a social norms problem: a community directly hostile to police tactics. When communities grow hostile, police have not just lost a valuable crime-fighting tool—they have gained a crime-fighting problem.

4. BROKEN WINDOWS IS NOW A CAUTIONARY TALE FOR POLICYMAKERS.

The social costs of broken windows make it a perfect example of a social policy that critically misunderstands social norms. Although well-intentioned, broken windows does not only disrupt street activity; it disrupts the reputation of local government as well. As a result, city governments that employed broken windows tactics now, to many of its citizens, look like broken city governments.[91] These governments must now recover from the devastating social costs of their actions and

---

[89] Miller, *supra* note 75, at 631.
[90] Fagan & Davies, *supra* note 78, at 499.
[91] Miller, *supra* note 75, at 686.

grapple with the irony that they have fostered the very disrespect for the law that they initially tried to avoid.

D. Recent innovations show promise for crime-fighting in the urban context.

Today, legal scholars are trying to reclaim the broken windows theory through a "more complex view" that "promotes construction of social networks that integrate community-level social processes with the regulation of crime and disorder."[92] In a particularly inspiring article, Eric Miller recommends that city governments strip the police force of the broken windows tactics that Giuliani championed.[93] Miller advocates giving this role to municipal workers: non-police city workers like crossing guards, bus drivers, subway operators, and park officials.[94]

In contrast to police officers, who often do not live in the areas that they police, many of these municipal workers work in the communities that they live in, "or travel so frequently through the community that they are identified with" that location.[95] Municipal workers are the community's neighbors, familiar faces, friends, relatives, and loved ones. This community integration, though seemingly trivial, serves a powerful purpose: it limits social backlash to low-level disorder policing.

When low-level order maintenance is integrated in this way, members of the community are less likely to perceive municipal workers as "an occupying soldier in a bitterly hostile country" when they combat low-level disorder.[96] In addition to being members of the same community (in which they may or may not be a familiar face), municipal workers are also less prone to employ the invasive tactics that humiliate community citizens and incite racial animus. Though municipal workers often wear uniforms, their uniforms do not usually include nightsticks or handcuffs, which dramatically reduces the potential for abuse and saber-rattling. Fur-

---

[92] Fagan & Davies, *supra* note 78, at 500.

[93] *See generally* Miller, *supra* note 75.

[94] *Id.* at 679.

[95] *Id.*

[96] *Id.* at 686 (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment,* 58 MINN. L. REV. 400 (1973–74)).

thermore, it would be odd for park janitors to stop-and-frisk random citizens, or for city bus drivers to rummage through every-third backpack at each bus stop.

In this way, municipal workers are incapable of many of the controversial tactics that ruined the original broken windows policy. But they still have an extraordinary ability to prevent the low-level disorders that broken windows combats: bus drivers and park janitors can encourage citizens "to pick up their trash, scoop up after their dogs, not congregate in a threatening manner on street corners, keep the noise down, and obey other consistent norms."[97] They can identify troublesome areas, act as caretakers for the poor and mentally ill, and clean up graffiti, one of the most visible broken windows in the city. As the "eyes and ears on the street," municipal workers can act as a "first defender" on city streets. Through verbal admonitions and clean-up, they can encourage the community to join in the policing effort without creating the legitimacy crisis that accompanies official police action.[98]

In addition to avoiding the legitimacy crisis, order policing by municipal workers may even be an important way to rebuild the reputations of police departments in post-broken window communities.[99] As Miller illustrates, "municipal officials are able to communicate the powerful message that quality-of-life issues matter and the government is taking it seriously, while simultaneously modeling appropriate norms of behavior in normatively fragmented communities."[100] Effectively, municipal officials are capable of serving two functions: as uniformed government officials (that are not prone to the violent excesses of police officers), they can model ideal policing behavior, and as non-police community members charged with enforcing the law, municipal workers are poten-

---

[97] *Id.* at 679–80.

[98] *Id.* at 664 ("This does not entail that the 'real' police do less policing, but that they do policing of a particular kind, one that avoids escalation and the minority perceptions of illegitimacy that accompany it.").

[99] *Id.* at 686 (arguing that enlisting municipal workers in role-based policing "confers substantive legitimacy upon both the manner of policing and the norms policed. Perhaps more importantly, it constitutes the community, with all its plural voices, as worthy of consultation and respect, and capable of self-regulation given the appropriate tools").

[100] *Id.* at 679.

tial paragons of citizen behavior. This duality makes municipal workers a powerful intermediary: municipal workers are not only capable of becoming an exemplar for how the city government should interact with its citizens, but also an exemplar for how citizens should interact with their government.

The latter is perhaps most apparent when violent crime does erupt in a community. In situations of high-level disorder, "[m]unicipal officials will not chase down and detain fleeing criminals caught in the act. This type of activity is outside their role."[101] Instead, municipal workers will have to alert and cooperate with the police investigating a violent crime, just like any other concerned citizen. In other words, they will be forced to cooperate with the police in ways that cities hope ordinary citizens would; their job description will entail being model citizens and examples in the community.[102]

Miller's proposal is an important contribution to social norms literature because it illustrates that policing loose-knit communities is not an all-or-nothing proposition. The choice policymakers face in a loose-knit community is not between forceful suppression and utter neglect. Instead, governments in loose-knit communities can and should deputize intermediaries to help police and model desired behavior. As the "eyes and ears on the street," these intermediaries can identify familiar causes of disorder that undermine the quality of life, combat their source, and notify the government when it gets out of hand. While not a solution for every problem, this sort of prophylactic strikes the proper balance between extralegal and legal norms. And while not a solution for every context, loose-knit communities should consider this approach before resorting to invasive police tactics.

PART III: THE INTERNET AS A CITY

One such loose-knit community is the Internet, which shares striking similarities with the city context. As illustrated below, due to its overwhelming size, frenetic environment, and anonymity capabilities, the Internet mimics the loose-knit feel of the

---

[101] *Id.* at 680.

[102] *Id.* at 679 ("Municipal officials often undertake the role of public policing within the mandate of their job titles.").

city. As a result of this interesting similarity, Internet policymakers should learn from city policing through analogy, pay heed to painful lessons learned from the broken windows experiment, and avoid invasive policing and surveillance on the Internet.

A. The Internet amplifies the aspects of the city that inhibit social norm growth.

1. BOTH CITIES AND THE INTERNET ARE DEFINED BY THEIR DENSE POPULATIONS.

While a formal definition of "city" is difficult to articulate,[103] one of its most striking characteristics is its number of inhabitants.[104] And in terms of population, the Internet is staggering. There are already over 1.8 billion Internet users worldwide,[105] and over one billion "publicly readable web pages."[106] In the United States alone, current Internet population estimates range from 165 to 210 million.[107] This is roughly 20 to 26 times the population of New York City.[108] And by all estimates, the Internet population is continuing to grow: aggregate world Internet data traffic grew 53% between 2007 and 2008,[109] and some researchers anticipate this traffic to grow 100% annually, possibly quadrupling by

---

[103] RALPH THOMLINSON, URBAN STRUCTURE: THE SOCIAL AND SPATIAL CHARACTER OF CITIES 37 (1969) ("The initial observation pertinent to defining a city is that neither social scientists nor governing bodies in various countries agree among themselves on a definition.").

[104] *Id.* ("A common approach is to specify a minimum number of inhabitants; above a certain number of residents, a community is called a city.").

[105] InternetWorldStats.com, World Internet Usage Statistics News and World Population Stats, http://www.internetworldstats.com/stats.htm (last visited April 27, 2010).

[106] A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 782 (2003).

[107] DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, CHINA'S ONLINE POPULATION EXPLOSION: WHAT IT MAY MEAN FOR THE INTERNET GLOBALLY . . . AND FOR U.S. USERS (2007), *available at* http://www.pewinternet.org/~/media//Files/Reports/2007/China_Internet_July_2007.pdf.pdf.

[108] U.S. Census Bureau, Population Estimates, http://www.census.gov/popest/cities/SUB-EST2008.html (last visited April 27, 2010).

[109] Jim Duffy, *Internet Traffic Growth Slows*, PC WORLD, Sept. 7, 2008, http://www.pcworld.com/article/150709/internet_growth_trends.html?tk=rss_news.

2011.[110] Given this robustness, the Internet not only imitates the size and pace of most urban centers; it exceeds them.

As a result, the Internet is often described in urban terms. Perhaps the Internet's most famous moniker, "the information superhighway," compares the Internet to the high volume road system that city-inhabitants use as transportation. Similarly, Internet "traffic" compares the conveyance of data and information to the conveyance of cars on city roads. Some have even tried to stretch the metaphor further: in 2008, the *New York Times* referred to users of video websites as "road hogs" capable of creating "Internet traffic jams."[111]

2. THE DENSE POPULATION OF CITIES CREATES THE APPEARANCE OF ANONYMITY, AND ON THE INTERNET, THIS APPEARANCE OF ANONYMITY IS AMPLIFIED.

Perhaps the most important similarity between the Internet and the city is the anonymity of its inhabitants. As demonstrated in Part II, the high population size and density in cities creates constant "stranger interaction" that fosters feelings of anonymity. This is amplified on the Internet because, in addition to an enormous population level, Internet users are not limited by their geographic space. Unlike a city-dweller, who might restrict stranger interaction to their street, block, or city limits, Internet users encounter strangers from all over the world at any given time. On the Internet, a "person in Alaska can have a conversation with a person in Japan about beekeeping in Bangladesh, just as easily as several Smyrna residents can have a conversation about Smyrna politics."[112]

B. The Internet has unique characteristics that make social norms growth even more difficult than in the city.

1. THE INTERNET HAS MORE STRUCTURAL ANONYMITY THAN THE CITY.

The effects of anonymity are amplified on the Internet because, unlike the city, anonymity is inherent in its structure. In a city, there

---

[110] Steve Lohr, *Video Road Hogs Stir Fear of Internet Traffic Jam*, N.Y. TIMES, Mar. 13, 2008, at A1.

[111] *Id.*

[112] Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005).

is nothing *structural* that makes its citizens feel anonymous, and there is nothing *inherent* in city sidewalks that makes citizens strangers to one another. It is only the constant barrage of stranger interaction on roads and sidewalks that fosters anonymity in a city, and no matter how anonymous these city interactions seem, they primarily take place face-to-face.

In contrast, the Internet usually lacks face-to-face interaction, taking anonymity one step further. This enhanced anonymity is largely "due to the nature of the technology," since Internet users interact with one another through an impersonal computer screen.[113] Known as interacting "remotely," Internet user identities are obscured: users can act without ever showing their name, face, height, weight, or age. Thus, unlike "real space," where "anonymity has to be created" with masks and surreptitious behavior, "in cyberspace anonymity is the given."[114]

2. VARIOUS TOOLS ENHANCE THE ANONYMITY THAT THE INTERNET CAN OFFER.

In addition to the natural remoteness of Internet technology, users can enhance their anonymity through various means. One such tool is the "anonymous remailer," which acts as a sterilizing intermediary between e-mail "senders" and "receivers." Under normal circumstances, an e-mail automatically embeds information that includes the sender's "Internet protocol address," which indicates the sender's location. But when a user sends an e-mail through an "anonymous remailer" service, it

> strips [the e-mail message] completely of the true sender's identifying information, and forwards the message to the email address specified by the sender. With some experience, a person can use anonymous remailers to send untraceable, truly anonymous messages.[115]

---

[113] du Pont, *supra* note 2, at 192, 197.

[114] LESSIG, *supra* note 7, at 33.

[115] du Pont, *supra* note 2, at 198.

In this way, anonymous remailers prevent e-mail recipients from learning about the e-mail sender's location.

While "anonymous remailers constitute the bulk of truly anonymous communication in cyberspace, there are other ways to achieve true anonymity" on the Internet.[116] One easy way is through a new Internet connection. Since e-mail messages typically embed information about the sender's Internet connection—and rarely any information about the computer used—Internet users can evade detection by simply transporting their laptop to a new connection. At each of these new locations, the same computer will connect with a *different Internet protocol address* ("*IP address*"). This means that the same Internet user will lose all identifying characteristics each time she travels to and from various free wireless networks in libraries, Internet cafes, and city parks—all on the same computer.[117] She effectively becomes a new Internet user at every city block.

Anonymous remailers and public access areas prevent people from discovering the true geography of Internet users. But Internet users' locations are not the only aspects obscured; Internet connections hide much more. On the Internet, users can conduct communication under self-fashioned screen names that mask their true identity. Perhaps the best illustration of this anonymity is what Neal Kumar Katyal calls "digital pseudonymity."[118] According to Katyal,

> Digital pseudonymity refers to the ability to cover one's true name while in cyberspace. For example, my e-mail signature may be nka9845@aol.com and my IP address may be a series of numbers that match only an ISP. Without the ISP's cooperation, it is nearly impossible to figure out who nka9845 is, and even more difficult to pinpoint nka9845's location in realspace.[119]

---

[116] *Id.*
[117] *Id.* at 199.
[118] Katyal, *supra* note 3, at 1047.
[119] *Id.*

A pen name writ large, digital pseudonymity allows users to hide their true identity. And since these digital pseudonyms are easy to create, one Internet user can even hide behind multiple identities. Neal Kumar Katyal may be nka9845@aol.com, but he may also be 5489akn@aol.com, user NKK123 at his online banking site, and even user_that_looks_nothing_like_Katyal@aol.com. There are virtually no limits to the number of digital pseudonyms that one Internet user can hold; users can have different pseudonyms for different purposes, multiple e-mail addresses, and various log-in nicknames. In this way, pseudonymity not only allows Internet users to be anonymous, but also duplicitous.

3. WHEREAS DEVIANCE DETECTION IS IMPAIRED IN THE CITY, IT IS NEARLY IMPOSSIBLE ON THE INTERNET.

This anonymity and duplicity, however, carries social consequences. As illustrated in Part II, anonymity strips city communities of deviance detection, and this severely debilitates many traditional social sanctions that curb crime. And since anonymity is magnified on the Internet, this debilitation is also amplified.[120] For example, returning to the vandalism hypothetical in Part II: if a city-inhabitant experiences damage to her property by a stranger, she will probably not know the stranger's name, the stranger's friends, or the stranger's address. And if the stranger were wearing a mask, she might not know the stranger's face. But "[e]ven masked or otherwise disguised criminals in realspace may unwittingly indicate their height, race, voice, and now their DNA."[121] The victim of a city crime will probably be able to help police provide a witness sketch or a rough idea of the stranger's physical characteristics.

This is not necessarily true on the Internet. On the Internet, a stranger's physical characteristics are generally unknown. For that matter, the stranger's location may be unknown; he could be miles (if not continents) away. Unlike city-inhabitants, Internet users only disclose the information they *choose* to disclose, and if they prefer,

---

[120] A. Michael Froomkin, *Anonymity in the Balance*, *in* DIGITAL ANONYMITY AND THE LAW: TENSIONS AND DIMENSIONS 5, 7 (C. Nicoll et. al. eds., 2003) ("Anonymous communication is a great tool for evading detection of many varieties of illegal and immoral activity.").

[121] Katyal, *supra* note 3, at 1047.

they can even masquerade as someone that they are not. Internet users "do[] not have technical capability, the legal authority, the energy, the time, and/or the resources to authenticate the many identities and [pseudo]nyms [they are] deal[ing] with,"[122] crimes on the Internet "are almost always invisible"[123] to the communities they arise in. On the Internet, "you can park in a suburban street, use an open wireless access point to commit an online crime, and drive away before anyone notices."[124]

4. DIFFICULTIES WITH DEVIANT DETECTION BECOME COMPOUNDED BY THE INTERNET'S TOLERANCE FOR MULTIPLE IDENTITIES.

Since a crime can be committed on the Internet "before anyone notices," anonymity on the Internet devastates social norms policing because enforcement cannot operate until someone in the "Internet community" takes "notice" of deviant behavior. But even if every single user in the Internet community knew that definitely_not_Philip_Wells@aol.com had committed a crime on the Internet, social norms enforcement would have very little bite; "definitely not Philip Wells" could simply change his e-mail address.

Certainly, Internet users could warn others to avoid "definitely not Philip Wells" (negative gossip), shun "definitely not Philip Wells" from all communication and connections (ostracism), or even ban the Internet protocol address that "definitely not Philip Wells" committed the crime from. But these sanctions would exact harm only on the screen name and not the person himself. After committing an Internet crime, a user could avoid social sanctions entirely by registering a new screen name and logging in from a new location. For example, to obtain a new e-mail account from Google's "Gmail" service, users merely need to state their first and

---

[122] Roger Clarke, *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice* (1999), http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

[123] Katyal, *supra* note 3, at 1109.

[124] Richard Clayton, *Anonymity and Traceability in Cyberspace*, COMPUTER LABORATORY TECH. REPORTS: UCAM-CL-TR-653, 12 (November 2005), *available at* http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf.

last name and country location.[125] Google does not ask for other distinguishing characteristics, like age or street address, and has little means of verifying that users have input their actual first and last names.[126] Registering users can easily lie about their disclosures to Google. Accordingly, in a matter of clicks at an Internet café, "definitely not Philip Wells" could quickly start operating as "definitely_not_the_criminal_you're_looking_for@gmail.com" and shed the negative reputation of his previous pseudonym—even if the entire Internet community were aware of his actions.

These actions need not even be duplicitous: some Internet users may choose to divide their social and professional identities with separate screen names and separate accounts for non-criminal reasons. Today, it is not uncommon for Internet users to have a different work e-mail address than their personal address; this keeps respective inboxes organized and uncluttered. But even these benign multiple identities provide other Internet users with a myopic perspective that inhibits the ability for social norms to constrain deviant behavior. For example, a merchant who experiences a particularly pleasant interaction with philip.a.wells@gmail.com on an auction website may not realize she is dealing with pw@work.com during a later transaction. Even if the merchant would have hoped to retain philip.a.wells' business with a discounted deal, the multiple identities may prevent philip.a.wells' reputation from carrying over. These multiple identities are an obstacle to rewarding cooperative behavior as much as they are an obstacle to deterring bad behavior.

In game theory terms, anonymity, multiplicity (and, at times, duplicity) create imperfect information on the Internet, which prevents even repeat players from realizing that they are engaging in iterated play. Under normal circumstances, game theory states that repeat players engaged in iterated play are constrained by reputation because each player knows that he or she will encounter the opposing party again. But on the Internet, since pseudonyms can be changed so easily, repeat players cannot learn from previous interactions because they do

---

[125] Google.com, Create a Google Account – Gmail, http://mail.google.com/mail/signup.

[126] du Pont, *supra* note 2, at 198–99 ("Although these services ask for the user's name and address, this information is rarely verified.").

not realize that they have already met their opposing party before. In this way, "[g]ame-theory analysis demonstrates that there are inherent limitations to the effectiveness of reputation systems when people can start over with new names."[127]

C. GIVEN THE SIMILARITIES BETWEEN THE INTERNET AND THE CITY, INTERNET POLICYMAKERS SHOULD PAY HEED TO THE HISTORY OF URBAN CRIME-FIGHTING.

As illustrated above, the Internet shares important similarities with the city, including a dense population, overwhelming size, and anonymity, which contribute to the degradation of social norms.

These factors make the city's public spaces an important lens with which to view "publicly available" websites on the Internet.[128] Unlike the Internet, the city is an ancient entity. For centuries, societies around the world have grappled with social causes of crime in densely populated public areas. Some anti-crime policies have worked, some have failed, and others—like broken windows policing—remain extremely controversial with mixed results. This rich history, in tandem with the similarities between the Internet and the city, offer many useful lessons for Internet policymakers.

Admittedly, the analogy between the city and the Internet is not perfect. Cities are visible, physical entities limited by space and geography; the Internet is an invisible, computer-created "space" limited only by technology and the imagination of its users. The Internet is

---

[127] Paul Resnick, Richard Zeckhauser, Eric Friedman & Ko Kuwabara, *Reputation Systems*, COMMUNICATIONS OF THE ACM, December 2000, at 45, 48, *available at* http://delivery.acm.org/10.1145/360000/355122/p45-resnick.pdf?key1=355122&key2=3711217621&coll=GUIDE&dl=GUIDE&CFID=77697643&CFTOKEN=25758131.

[128] As stated above, this argument limits the "Internet" and the "city" in terms of its public spaces: streets, sidewalks, and restaurants in cities and "publicly accessible" websites on the Internet. These publicly accessible websites include Internet newspapers, commercial websites, blogs, and "peer-to-peer" and social networks; they do not include encrypted message boards and password-protected "invitation only" website forums. This note is agnostic as to whether these private websites on the Internet, like covert club meetings in cities, can create robust anti-crime social norms. But this limit *only strengthens* this note's insistence that governments should avoid a "one-size-fits-all" approach to policing cyberspace and should carefully calibrate policing depending on the social norms residing in each website community, private or not. *See supra* note 30.

not a place where skyscrapers rise, people sleep, and rats infest. In fact, the Internet is not really a "place" at all; it is simply a means of communication.[129] At first glance, these differences might tempt observers to treat the Internet and cities as *sui generis*.

But the analogy is quite apt with respect to social interaction. At any given moment on the Internet, users may be picking up the newspaper, sending mail to loved ones, buying their groceries, browsing for books, and even perusing pornographic material. In other words, on the Internet, people behave much as they would on a densely-populated city block. And while some differences persist, both Internet users and city-dwellers can do all of these tasks (1) quickly (often within an hour), (2) with ease, and (3) without being publicly recognized by others in the process.

These similarities make the history of crime-control in cities, such as the cautionary tales of broken windows and other counterproductive city policies, useful for developing Internet policy. Perhaps those who do not remember the past are not doomed to repeat the same mistakes; they are merely doomed to repeat them in different and analogous contexts. We should recognize that lessons from the past may be applicable to a variety of contexts, and that experimental urban crime policies provide critical lessons for Internet policing.

PART IV: PREVIOUS ATTEMPTS TO REGULATE THE INTERNET

Given the similarities between cities and the Internet, some scholars have tellingly advocated for broken windows policies in the Internet context, as discussed below. But just as broken windows provoked legitimacy concerns for city law enforcement agencies, a broken windows Internet policy and oppressive Internet tactics could bring about a nationwide legitimacy crisis for law enforcement.

---

[129] *See* Katyal, *supra* note 3, at 1111 ("In cyberspace, however, there are no geographic areas or boundaries."); *see also* Mark Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 523 (2003) ("As a technical matter, of course, the idea that the Internet is literally a place in which people travel is not only wrong but faintly ludicrous. No one is 'in' cyberspace. The Internet is merely a simple computer protocol, a piece of code that permits computer users to transmit data between their computers using existing communications networks.").

A. Crime and deviant behavior on the Internet is becoming a serious public concern.

Online crime has become a serious concern because remoteness, anonymity, and multiplicity on the Internet make it difficult for social norms to develop and thereby police certain undesirable behaviors. By all accounts, this fear is not completely unfounded: crime on the Internet has cost Americans over $8 billion between 2007 and 2009.[130]

These crimes are varied, and include attacks on individuals, corporations, and governments alike.[131] Even President Barack Obama apparently fell victim to hacking: in 2008, "online intruders" penetrated his campaign website and "rummaged through e-mails, travel plans, and other files."[132] But perhaps the most terrifying incidents have revolved around vicious, individualized attacks against ordinary citizens. Deviant behaviors such as cyber-bullying, cyber-stalking, and trolling—when Internet users embarrass, harass, and torment other users—illustrate the chilling dangers of impotent social norms.

In November of 2007, a suburban mother named Lori Drew masqueraded as a teenage boy on MySpace, using a fake screen name to flirt and later torture her daughter's 13 year-old classmate, Megan Meier.[133] Claiming that she was simply trying to discover whether Megan was gossiping about her daughter, Ms. Drew sent a series of cruel messages that eventually led to Megan's suicide.[134] Ms. Drew's "cyber-bullying" eventually earned her a federal conviction—the first of its kind.[135]

In another particularly graphic case, Jason Fortuny, a self-described online "troll" who enjoys "pushing people's buttons,"

---

[130] Randy James, *A Brief History of Cybercrime*, TIME, June 1, 2009, http://www.time.com/time/nation/article/0,8599,1902073,00.html.

[131] *Id.* (citing attacks against Barack Obama, Sarah Palin, the Pentagon, eBay, and university students, among others).

[132] *Id.*

[133] Jennifer Steinhauer, *Woman Found guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 26, 2008, at A25; Schwartz, *supra* note 1, at MM24.

[134] Steinhauer, *supra* note 133; Schwartz, *supra* note 1.

[135] Steinhauer, *supra* note 133; Schwartz, *supra* note 1.

posted a deceptive personals ad in 2006.[136] Disguised as a woman, Fortuny claimed to seek a "str8 brutal dom muscular male" in the Craigslist online dating section.[137] When more than one hundred men responded to the post, Fortuny posted their names, pictures, e-mail addresses, and phone numbers to his public website.[138] In an interview with the *New York Times*, Fortuny listed off the pain exacted: two men lost their jobs, and "at least one, for a time, lost his girlfriend."[139] Another filed an invasion-of-privacy lawsuit against Fortuny in Illinois.[140] Fortuny, for his part, is remorseless.[141]

Unfortunately, there are many more examples. In 2007, a man lured a 24 year-old woman to his house with a false Craigslist request for a babysitter, and shot her, according to prosecutors, "so he might experience what it felt like to kill."[142] In 2009, prosecutors claimed that Philip Markoff pretended to solicit prostitution on Craigslist's "erotic services" webpage, using this pretense to kidnap, rob, and in one case, kill, his victims.[143]

These attacks are all startling, but they also share a common thread: each exploited the Internet's inability to foster social norms. Manipulating the vulnerabilities of cyberspace, each of these predators used anonymity and duplicity to elude detection. In a non-Internet setting, it would have been extraordinarily difficult for Lori Drew to pose as a teenage boy and Jason Fortuny as a sexually explorative woman. Aside from obvious physical obstacles, the social pressures of etiquette and peer scrutiny would have largely removed the opportunity for either Drew or Fortuny to undertake their charades.

Of course, bullying and invasions of privacy existed long before computers; these crimes would exist with or without the Internet. But the ineffectiveness of social norms on the Internet makes these

---

[136] Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES, Nov. 26, 2008 at A25.

[137] Schwartz, *supra* note 1.

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id.* ("'I'm not going to sit here and say, 'Oh, God, please forgive me!' so someone can feel better,' Fortuny said, his calm voice momentarily rising.").

[142] *Craigslist Killer Gets Life Without Parole*, CBS NEWS, Apr. 1, 2009, http://www.cbsnews.com/stories/2009/04/01/national/main4911771.shtml.

[143] Matt Collette, *Charges Expand in Hotel Killing*, BOSTON GLOBE, June 22, 2009.

crimes much easier to commit. In real life, if an Internet hacker had hovered around the then-candidate Obama's street mailbox with a crowbar, he would have had to overcome public suspicion—and likely a 9-1-1 call—from Hyde Park neighbors. Behind his computer, however, nothing kept him from hovering around Obama's e-mail mailbox. And while in real life, Lori Drew's teenage boy disguise would have immediately triggered social backlash from other mothers, neighbors, and perhaps her own family ("Why are you running off in a wig and talking to my classmate, Mom?"), her cyberspace disguise merely took a few keystrokes and did not raise any eyebrows until after the crime had been committed.

B. In response to sensational crimes, legal scholars are beginning to advocate for broken windows policing on the Internet.

The above examples are compelling reminders of the Internet's vulnerability to crime and the need for swift action. Underscoring this need, on May 29, 2009, President Obama appointed a "cyber czar" to combat "the growing problem" of Internet crime.[144] Though noble, swift reactions have led some scholars to rashly reapply failed urban crime-fighting to the Internet. For example, in Neal Kumar Katyal's article, *Criminal Law in Cyberspace*, Katyal specifically prescribes "trendy theories of enforcement such as Broken Windows policing" to counter the Internet's social norm vacuum.[145] According to Katyal, because impaired social norms make the cost of committing crimes on the Internet very low, "law enforcement must punish, rapidly and powerfully, those crimes that produce the most visible social disorder in cyberspace."[146] The thrust of Katyal's argument is appealing: since crimes in the real world take the time, effort, and expense of careful planning and execution and cybercrimes merely require a key stroke, policymakers should raise the costs of committing cybercrime. One way Katyal proposes is disproportionate sentencing.

> [I]nstead of treating all crime as equal, law enforcement should attempt to inflict disproportionately

---

[144] James, *supra* note 130.
[145] *See* Katyal, *supra* note 3, at 1077.
[146] *Id.* at 1110.

> heavy punishments upon those crimes that create the most visible, or otherwise evident, social disorder in cyberspace. Doing so will avoid complementarity problems, such as copycat crimes or crimes committed because hackers' tools are easily accessible, and will help reassure the public and industry that cyberspace is safe.[147]

Although well-intentioned, Katyal's disproportionate Internet sentencing proposal echoes the failed urban crime-fighting policies of the 1990s. As stated above, broken windows targets the most "visible, or otherwise evident social disorder[s]," but fails to account for social and racial disparities that such a crackdown might create. The result of this oversight was a crippling legitimacy crisis in various urban communities that created a profound disrespect for the law in the areas that needed it most.

Admittedly, cyber-sentencing will probably not create the racial animus that infected cities. Unlike the city, where racial groups tend to be geographically concentrated and segregated, the Internet has little geography.[148] But that does not mean that severe crackdowns on certain Internet crimes will not disproportionately affect other discrete populations, including certain age groups. This is especially true for music copyright piracy, an Internet broken window that is prevalent on college campuses.[149]

---

[147] *Id.* at 1113.

[148] *See* David R. Johnson & David Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1995–96) ("Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries."); Katyal, *supra* note 3, at 1004.

[149] *See* Amy Harmon, *Recording Industry Goes After Students over Music Sharing*, N.Y. TIMES, Apr. 3, 2003, at A1; *see also Industry Pressure on Music Piracy*, N.Y. TIMES, Mar. 1, 2007, at C5 ("'The theft of music remains unacceptably high and undermines the industry's ability to invest in new music,' said Mitch Bainwol, chairman and chief executive of the [recording industry] association. 'This is especially the case on college campuses,' he said."); Matt Richtel, *Developing Technology for Internet Music Sales*, N.Y. TIMES, Apr. 17, 2000, http://partners.nytimes.com/library/tech/00/04/biztech/articles/17neco.html ("College students, while not the only ones to blame, have become piracy's poster children.").

B. The case study of illegal music piracy illustrates the dangers of a broken windows policy on the Internet.

Music piracy is a crime that has both civil and criminal penalties, and is rampant in both the real world and on the Internet.[150] Compared to cyber-bullying and murder, music piracy may seem rather innocuous. But as the broken windows theory mandates, music piracy should be relentlessly crushed to demonstrate to trolls and cyber-bullies that they will be punished.

In the case of online music piracy, "[c]ollege campuses, the record industry says, have become far and away the prime locus" of criminality.[151] If the federal government took Katyal's recommendation and enacted disproportionately harsh penalties for online copyright crimes (compared to the offline form of the same crime), college-age citizens would pay the price with their pocketbooks and their liberty. Such disproportionate enforcement, intended to "reassure the public and industry that cyberspace is safe,"[152] would instead disproportionately rip college-age students from their communities, penalize younger age-groups, and once again "send conflicting messages to young people: our supposedly fair and equal justice system treats them differently" for the same crimes.[153]

Draconian broken windows sentencing may deter online piracy crimes in the short-run. But in the long-run, such measures would inflame age animus and create yet another legitimacy crisis for crime-fighters. And whereas cities might have to grapple with broken windows legitimacy costs for several blocks, the entire nation would be throttled by an Internet-based legitimacy crisis. Cyber-sentencing would foster this animus in every single city, in every single state, and would infect an entire generation of Americans with a dangerous disrespect for the law. Just as

---

[150] *See generally* Kim F. Natividad, *Stepping It up and Taking It to the Streets: Changing Civil & Criminal Copyright Enforcement Tactics*, 23 BERKELEY TECH. L.J. 469 (2008).

[151] Harmon, *supra* note 149.

[152] Katyal, *supra* note 3, at 1113.

[153] Charles J. Ogletree, Jr., *The Burdens and Benefits of Race in America*, 25 Hastings Const. L.Q. 219, 229 (1998) (discussing the disproportionate impact of sentencing for crack cocaine on urban minority communities).

urban feelings of anonymity are amplified on the Internet, the urban legitimacy crises would be amplified as well.[154]

Music piracy is merely one example for which Katyal's higher sentencing proposal would carry unintended social costs.[155] If applied to other Internet crimes, these costs could—and likely would—pose similar legitimacy crises wherever demographic differences existed between online and offline forms of the same crime. Demographic differences do not even need to be *actual differences*; *perceived* disparities are enough to cultivate perceptions of unfairness. For instance, in the case of music piracy, as long as younger Americans *feel* unjustly targeted by higher online sentences—regardless of the actual offline/online statistical breakdown—that perception is enough to cultivate a profound distrust for Internet policing. Legitimacy is based on perception, not on mathematics.

If policymakers inflict harsher penalties for an online crime than its offline counterpart—and these penalties disproportionately impact certain age, race, or economic communities—well-intentioned penalties would expose the justice system to accusations of animosity that, even when incorrect, would undermine social support for the entire legal system. This would occur in large part because such incongruities make it glaringly apparent that criminal punishment does not merely reflect the moral approbation of a particular crime, *but also something else*. Even though this "something else" may be a careful calibration to match criminal methods with their relative "perpetration costs" (as Katyal envisions),[156] this unfamiliarity would breed contempt for an already embattled Internet criminal policy.

---

[154] Tellingly, the recording industry has recently stopped filing lawsuits for music piracy because it created "a public-relations disaster" when it targeted, amongst others: college students, teenagers, and several single mothers. Sarah McBride, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1; Alison Go, *RIAA to Hold off on Mass Suits*, U.S. NEWS & WORLD REPORT, Dec. 19, 2008, http://www.usnews.com/blogs/paper-trail/2008/12/19/riaa-to-hold-off-on-mass-lawsuits.html ("The Recording Industry Association of America confirmed Friday it will no longer pursue mass lawsuits against copyright infringers, which includes a significant number of college students . . . .").

[155] Another example may be computer hacking, which Katyal himself posits may be committed primarily by teenagers. Katyal, *supra* note 3, at 1011.

[156] *Id.* at 1114.

Policymakers and legal scholars must not re-learn the lessons of broken windows on the Internet. This policy has already proven counterproductive in cities and threatens the very vitality of the criminal justice system. On the Internet, where legitimacy stakes are even higher, law enforcement cannot afford another mistake; nor should it.

1. AGGRESSIVE POLICE TACTICS WOULD HAVE NEGATIVE CONSEQUENCES ON INTERNET POLICY.

Internet broken windows sentencing would exact a serious cost on the criminal justice system. But the cost would multiply if policymakers blindly extended broken windows *police tactics* to the Internet as well. Unfortunately, policymakers seem poised to do so: the federal government has consistently advocated an invasive approach to Internet policing through e-mail surveillance, as discussed below.[157]

In the city, broken windows policymakers both increased sentences for low-level crimes and employed invasive street techniques (like stop-and-frisks) to fight crime, but such an aggressive approach reaped large numbers of warrantless arrests,[158] unconstitutional searches,[159] and questionable ordinances[160] that undermined its legitimacy. In a startling similarity, the federal government has duplicated this bellicose behavior on the Internet.[161] Federal officials have already admitted that law enforcement has wielded anti-terrorism laws to "improperly, and sometimes illegally," obtain information about businesses and individuals on the Internet.[162] Even where law enforcement officials have acted *legally*, they have often over-stepped their bounds: in a 2006 report the Justice Department

---

[157] *See generally* Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1; *Bush Signs Controversial Surveillance Bill*, CBS NEWS, July 10, 2008, http://www.cbsnews.com/stories/2008/07/10/politics/main4248847.shtml?source=RSSattr=Politics_4248847.

[158] Fessenden & Rohde, *supra* note 48.

[159] Newman, *supra* note 48.

[160] *See* City of Chicago v. Morales, 527 U.S. 41 (1999) (overruling the Chicago anti-loitering ordinance as unconstitutionally vague).

[161] Froomkin, *supra* note 120, at 30.

[162] David Stout, *F.B.I. Head Admits Mistakes in Use of Security Act*, N.Y. TIMES, Mar. 10, 2007, at A1 (regarding the now-expired Patriot Act).

admitted that there were "more than 100 violations of federal wiretap law . . . by the Federal Bureau of Investigation ["FBI"], many of them considered technical and inadvertent."[163]

These are troubling disclosures in light of the lessons learned from broken windows policies. But in a *New York Times* article entitled *F.B.I. Gained Unauthorized Access to E-Mail*, FBI intelligence officials exhibited startling indifference to this activity: "'It's inevitable that these things will happen. It's not weekly, but it's common.'"[164] And when given the chance to admonish these officials, Congress declined, instead approving even more expansive surveillance five months later.[165] In this 2008 law, which amended the Foreign Intelligence Surveillance Act of 1978,[166] Congress implicitly approved of the FBI's actions by providing "the executive branch broader latitude in eavesdropping on people abroad and at home who it believes are tied to terrorism," reducing "the role of a secret intelligence court in overseeing some operations."[167]

PART V: VILLAGE-BASED INTERNET POLICING

Internet policymakers should learn from the cyber-city analogy. Instead of reliving the broken windows mistakes of the past, Internet policymakers should fashion a new approach that incorporates the painful lessons learned by city law enforcement. Specifically, the policymakers should harness a "village-based" approach based on Eric Miller's "deputized intermediary" approach to urban crime, which involves enlisting municipal workers to act as a bridge between citizens and the formal police department.[168]

At first glance, Miller's proposal to deputize municipal park and transit workers seems inapplicable to the Internet. After all, there are no roving Internet custodians or train conductors that help users navigate cyberspace. But in a more general sense, there *are* important intermediaries between governments and Internet users:

---

[163] Eric Lichtblau, *F.B.I. Gained Unauthorized Access to E-Mail*, N.Y. TIMES, Feb. 17, 2008 at A1.

[164] *Id.*

[165] Lichtblau, *supra* note 157.

[166] 50 U.S.C. § 1801 (2008).

[167] Lichtblau, *supra* note 157.

[168] *See supra* notes 92–102 and accompanying text.

the people who own and manage Internet websites and peer-to-peer networks ("web-administrators"). Like Miller's municipal workers, web-administrators operate in contained "spaces"—their own websites—and closely interact with Internet users who use their sites.[169] From this intimate position, web-administrators are capable of acting as the "eyes and ears" within their own websites, monitoring their respective communities, combating cyber-bullying and illegal activity, and notifying the government when it gets out of hand. And since web-administrators can manipulate websites through its underlying code, they are remarkably dynamic actors in the Internet community. Through coding, web-administrators are not merely capable of interposing themselves between and among Internet users, but are also able to react to their users and change the underlying code accordingly. In this way, web-administrators do not just patrol Internet "streets;" they create them.[170]

As such flexible actors, web-administrators can dramatically change the way in which users act on the Internet. Through various techniques discussed below, web-administrators can structure their

---

[169] Some scholars have emphasized that governments enlist another intermediary—Internet service providers ("ISPs")—to police the Internet. *See, e.g.*, Katyal, *supra* note 3, at 1003, 1007–08, 1013, 1030, 1036. But as Katyal himself notes, "[p]lacing burdens on ISPs risks balkanizing the net and inducing ISPs to purge risky users." *Id.* at 1100. Since ISPs control access to *the entire Internet* and not simply a "contained" area like web administrators, ISPs are not only the gate-keepers of one site: they are the gate-keepers to *every site*. This makes ISPs overly-powerful government deputies and creates the possibility that "overzealous" ISPs "will suppress [First Amendment] protected speech" on the Internet by banning suspect customers altogether on the Internet. Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 33 (2007). This problem is compounded by the fact that, unlike websites, Internet users often lack ISP alternatives (e.g., college students are subject to one ISP—their university). *Id*. at 34–35. This would make it very difficult for Internet users to "discipline" overzealous or renegade ISPs by choosing a competitor: there is no other option. *See id*. In contrast, web-administrators face constant competition: Internet users can quickly switch away from suppressive or undesirable social networking sites.

[170] Admittedly, this solution only applies to "publicly available" Internet websites. Publicly unavailable websites, including "invitation-only" encrypted and secretive message board communities—like non-public spaces in cities—may require different forms of policing. But this limit only accentuates the argument: Internet policing must be carefully tailored depending on the social dynamics inherent in each website. *See supra* notes 30, 128.

websites not only to monitor their visitors, but also to facilitate more intimate social contact. In other words, web-administrators can pave their "streets" to feel less like anonymous cities and more like electronic Shasta County ranch villages. Put in terms of Ellickson's social norms, web administrators can make Internet users act less like loose-knit community members and more like close-knit community members where social norms can operate.

A. Web-Administrators can use a variety of techniques to build self-policing on their websites.

1. OPT-IN DISCLOSURES CAN DRAMATICALLY ALTER SOCIAL NORMS ON WEBSITES.

One powerful technique in a web-administrator's arsenal is the sign-in page. By requiring visitors to voluntarily "sign up" to participate in a web community, websites can encourage Internet users to voluntarily surrender their anonymity. Websites like eBay,[171] Facebook,[172] and Yelp[173] do this to varying degrees on their registration pages.

Registration discrepancies between these sites reflect expected use: eBay requires a full mailing address because it anticipates users will be mailing goods to and from one another after an auction; Yelp requires a zip code because it expects users will want to read and review restaurants in their area; and Facebook requires a birthday to allow users to contact each other on that day. Notably, however, all four websites require a full name.

This act of full name registration—a requirement for entering each website community—is a powerful hurdle. As Xeni Jardin, co-editor of the popular weblog BoingBoing.net, noted in an interview with PBS, registration curtails deviant behavior because

---

[171] *See* Ebay Home Page, http://www.ebay.com/ (last visited Apr. 27, 2010). Ebay requires a full name, desired screen name, mailing address, e-mail address, and telephone number.

[172] *See* Sign Up For Facebook, http://www.facebook.com/r.php (last visited Apr. 27, 2010). Facebook requires a full name, e-mail address, sex, and birthday.

[173] *See* Yelp Sign Up, https://www.yelp.com/signup (last visited Apr. 27, 2010). Yelp requires a full name, mailing address (zip code), and e-mail address.

> [An Internet user] could even use a fake name[,] but just that act of registering with a site . . . sort of puts a lid on the drive-by shootings (as people call them)—when people just go to a comment section and write profanity or obscene things . . . It kind of keeps that a little bit in check.[174]

Website registration keeps Internet users "a little bit in check" because it acts as a visible reminder that users will be held accountable for their actions in web communities; their name, just as the "family names" of Shasta County, will be at stake. And instead of a legal boilerplate and "terms and conditions" that Internet users might overlook or ignore, this registration requires *affirmative action* on the part of Internet users.

2. REPUTATION SYSTEMS CAN RECREATE REPEAT-PLAY AMONG INTERNET USERS, THOUGH WITH MIXED SUCCESS.

Admittedly, registration hurdles are not enough on their own. Determined deviants like Lori Drew can still input false names or continually re-register under duplicitous pseudonyms. In response to this problem, sites like eBay have constructed complicated reputation systems to encourage users to invest in their online identity. On eBay, web administrators encourage users to rate each other after each transaction. Users are able to select a rating (1, 0, or -1) and to leave comments ("This transaction was very honest and fair. I look forward to doing business with her again!"). This rating is then attached to a running total and displayed visibly next to the user's eBay screen name at all times. This casts an ever-lengthening shadow on each pseudonym and provides users with empowering information with which to screen potential sellers/buyers.

In social norm terms, eBay's reputation system creates close-knit intimacy because it provides the social control ("negative ratings") and information necessary for such control ("visible ratings and past comments") to create "trustworthiness" and "good faith dealing" between users. Like the cattle ranchers in Shasta County, eBay users feel compelled to transact honestly in order to avoid social retribution. On eBay,

---

[174] Interview by Jeffrey Brown with Xeni Jardin, Co-Editor, BoingBoing.net (Jan. 24, 2006), *available at* http://www.pbs.org/newshour/bb/media/jan-june06/post_1-24.html.

this retribution is not merely emotional: eBay buyers may demand lower prices or better terms to compensate for the risk of dealing with a disreputable seller. And if a seller's rating is low enough, buyers may avoid the user altogether. In this way, eBay's reputation system does not merely make deviant users feel guilty for their actions; it makes them unprofitable as well.

Although reputation systems are a powerful way to facilitate social norms on websites, they contain certain drawbacks. One is the "barrier to entry" that the system erects against new users. New eBay users—who begin with no feedback history—"should always be distrusted until they have somehow paid their dues, either through an entry fee or by accepting more risk or worse prices while developing their reputations."[175] Through no fault of their own, new eBay users will be treated (and penalized) as deviants until they can establish a reputation on the website. These unfair penalties—like the unfair broken windows targeting in cities—can foster indignation that discourages members from rating other users or from using the site entirely.

This struggle of "honest newcomers" is exacerbated by the fact that truly deviant eBay users can escape their negative reputations by merely registering a new screen name. The duplicity problem persists in reputation systems with easily obtained pseudonyms, and would tempt existing eBay users to treat newcomers even *more unfairly*, since they are more likely to be masquerading deviants. Working in tandem, newcomer penalties and duplicity threaten the credibility of reputation systems based on pseudonyms. Consequently, reputation systems like eBay are an interesting tool in the web administrator's social norms toolkit, but largely an incomplete one.

3. THE REQUIREMENT TO USE REAL NAMES ON INTERNET WEBSITES IS PERHAPS THE STRONGEST ANTIDOTE TO DEVIANT BEHAVIOR.

Some scholars have proposed that web administrators abandon pseudonyms altogether in favor of real names.[176] This was the decision of web administrators on Facebook,[177] the Internet's largest

---

[175] Resnick, Zeckhauser, Friedman & Kuwabara, *supra* note 127, at 48.

[176] *Id*.

[177] *See* Sign Up For Facebook, http://www.facebook.com/r.php (last visited Apr. 27, 2010).

social network,[178] where screen names are not allowed. On Facebook, unlike on other social networking sites like MySpace,[179] users are required to display their first and last names at all times. Real name registration raises the stakes: on Facebook, each user risks the reputation of his or her *legal name*. To prevent duplicity, Facebook further discourages name changes through a delayed confirmation process that takes "approximately 24 hours" to take effect.[180]

Admittedly, Facebook users could still *originally* try to sign up with a false name at registration.[181] Lori Drew could still attempt to register as a teenage boy; Jason Fortuny could still try to sign-on as a woman with exotic sexual interests.[182] But Facebook's administrators have assembled an array of other techniques that nurture social norms and discourage such fraudulent behavior. For example, through public visitor-to-visitor communication on user "walls," public "friend lists," and the ability to post photographs, administrators have made maintaining a fraudulent Facebook identity a full-time affair. On Facebook, users cannot create a false identity through re-registration alone; it requires the constant cultivation of a robust identity. This is due to the general social expectations that Facebook administrators have fostered: users are expected to use real names, post an accurate (if often flattering) mug shot, write noteworthy messages on other user walls (especially on birthdays), and maintain a list of friends. And if a user does not do so, this sends a signal to other Facebook users—like a low reputation

---

[178] Brad Stone, *Facebook Aims to Extend its Reach Across the Web*, N.Y. TIMES, Dec. 1, 2008, at B3; Mike Musgrove, *Facebook Passes MySpace with Global Boost*, WASH. POST, June 24, 2008, at D03.

[179] MySpace, http://www.myspace.com/ (last visited Feb. 26, 2010). The difference in social norms between MySpace and Facebook remain striking, and deserve further exploration. Since both are social networking sites but seem to yield very different social norms, these two websites indicate that social norms on the Internet do not depend on the purpose of a website, but rather the techniques website administrators employ.

[180] Facebook: My Account, https://register.facebook.com/editaccount.php (last visited Mar. 2, 2010).

[181] *See, e.g.*, Tresa Baldas, *Fake Online Profiles Trigger Suits*, NAT'L LAW J., June 2, 2008, *available at* http://www.law.com/jsp/article.jsp?id=1202421864062 (discussing various lawsuits in which students have created false Facebook profiles of their school administrators).

[182] *See, e.g.*, Schwartz, *supra* note 1 (reporting that Lori Drew used a MySpace account to cyber-bully a schoolchild as a teenage male and that Jason Fortuny masqueraded as a woman on Craigslist, seeking a "str8 brutal dom muscular male.").

score on eBay—that this user is an "odd duck" and possibly risky member to interact with. This makes masquerading on Facebook exceedingly difficult. Whereas some websites—like Lori Drew's MySpace page and Jason Fortuny's Craigslist posting—tolerate duplicity after a one-click transaction, Facebook requires a laborious online lifestyle.

These expectations, in addition to the real name requirement, inhibit deviant behavior because they create unavoidable accountability for Facebook users. Since user action is tethered to a real name and mug shot, any potential deviant must be willing to leave an enormous digital fingerprint.[183] For example, when a Facebook user posts a controversial message on another's wall, this message is published on the "mini-feed" of all of the recipient's friends and all mutual friends that the sender and the recipient share—possibly hundreds of social acquaintances. This makes deviance on Facebook akin to committing a crime in broad daylight, without a mask, wearing a very legible nametag and in front of a grandstand populated by family members and friends.

This "mini-feed" is a very harsh spotlight. And since this information reaches family members and friends instantaneously, this spotlight engenders very robust social controls. In response to deviant behavior, other users can quickly delete or reject the deviant's "friendship" (ostracism), warn others about the deviant (negative gossip), publicly berate the deviant on his or her "wall," subject the deviant to a "limited profile friendship," or even "flag" the deviant's profile for administrator review. And that is just on Facebook; with real name identities, friends can socially penalize the user *offline* as well.

Facebook's mini-feed gives the Internet a mini-feel, and this creates a major impact on user behavior. Facebook has effectively created an Ellicksonian "close-knit group": both the informal social control and information necessary for such control are broadly available to Facebook users. In this way, Facebook has effectively shrunk its portion of the Internet "city" into an electronic Shasta County "village" capable of self-policing through social norms.[184]

---

[183] *See generally* John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES, Nov. 29, 2008, at BU1.

[184] *Cf. id.* ("For most of human history, people have lived in small tribes where everything they did was known by everyone they knew," Dr. [Thomas] Malone [of

B. The stunning proliferation of social norms through voluntary disclosures indicates that government intervention may be unnecessary.

In light of the Internet's inherent anonymity, it is stunning that intimate social norms have developed on Facebook. But what is even more remarkable is *why* they have developed: users seem willing to give up their anonymity when given the chance. Facebook administrators have induced Internet users to *voluntarily* abandon their anonymity and willingly subject themselves to the social controls of their Facebook friends.

1. VOLUNTARY DISCLOSURES DIMINISH PRIVACY CONCERNS.

Interestingly, Internet users seem seduced by the very complex social arrangements—like Facebook—that police their own actions. But while this groundswell attraction increases the ability for social norms policing, the required "entry toll" to these websites exacts a privacy cost: Internet users are revealing their real names to a website, often a corporation, and to all of its "customer" users. These websites can then access this information, sell it to others, or even tailor online advertising to the Internet user's demographic.

Importantly, however, these privacy concerns are much fewer than those created by alternative Internet policing techniques because they are created voluntarily: users choose whether or not to join these websites. Unlike *post hoc* court subpoenas won in the crucible of expensive litigation, in which information is wrestled from an unwilling Internet user and made public,[185] Facebook (and sites like it) provides users with the deliberate choice of whether to join. Nothing, for example, prevents privacy-minded Internet users from willfully rejecting Facebook's burgeoning network in favor of a monastic Internet existence. Unlike controversial police wiretapping conducted without the *knowledge* of the

---

M.I.T.] said. "In some sense we're becoming a global village. Privacy may turn out to have become an anomaly.").

[185] *See, e.g.*, Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008).

Internet user, Internet users know which information Facebook has and does not have access to—they typed it in themselves.[186]

2. VOLUNTARY DISCLOSURES DIMINISH POLICING COSTS.

The voluntary nature of Facebook's social norm growth not only diminishes privacy costs; it minimizes Internet policing costs as well. Without coercion and tax dollars, users already police their own pages, monitor others through the "mini-feed," chastise or ostracize Facebook friends when their behavior is inappropriate, and report unmanageable problems to Facebook administrators.[187] In a sense, due to various transparency features implemented by Facebook administrators, Facebook users are now mending their own broken windows. This is a beautiful development, and as Facebook explores new ways to extend its community (and revenue) to reach "sites that have been entirely unsociable thus far," Facebook social norms—and subsequent law-abiding behavior—may be poised to blossom across the Internet, including emergent sites like Twitter, the news aggregator Digg, and the online video website Hulu.[188]

C. When website registration requirements and voluntary disclosures fall short, websites should act like municipal workers.

Admittedly, extreme deviance on Facebook, like sexual predation and cyber-bullying, may not be completely curtailed by these transparency features, especially if all of a deviant's Facebook

---

[186] Admittedly, Facebook's privacy policies are the source of some controversy. *See* Brad Stone, *Facebook's Privacy Changes Draw More Scrutiny*, N.Y. TIMES BITS, Dec. 10, 2009, http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny/ . And while Facebook users may object to revealing the information they have typed into their Facebook profiles, this does not change the fact that the user originally opted to include this information in the Facebook universe (privacy issues aside). As the *New York Times* notes, "[t]hose who are particularly upset with the quasi-public aspects of Facebook's service can, of course, take advantage of one killer Facebook feature: not using it at all." *Id*.

[187] Juan Carlos Perez, *Three Minutes with Facebook's Privacy Chief*, PC WORLD, Feb. 10, 2008, http://www.pcworld.com/article/142324/three_minutes_with_facebooks_privacy_chief.html ("We've found that users are some of the best reporters on that, and our reporting infrastructure is extraordinarily effective in removing inappropriate content quickly and in holding those users who attempt to post them responsible by cutting off their account.").

[188] Stone, *supra* note 178.

"friends" are other predators or bullies. Under these circumstances, the government should enlist web administrators, like Miller's municipal workers, to detect and disrupt these counter-communities.

Like Miller's municipal workers, web administrators are well-equipped to identify troublesome activity, suspend or block deviant users, and clean up offensive e-graffiti on "walls," "message boards" and "comment forums." Importantly, these techniques would combat disorder without creating the legitimacy crisis that would otherwise accompany official police action. Additionally, since enforcement actions would be taken by private third parties and not by the government, policing would not incur any tax monies to police online behavior—it would be costless to taxpayers.[189]

A website-police partnership would be an efficient and effective way to police robust Internet communities. Facebook seems to recognize this, and has already begun building relationships at the state level.[190] Facebook reports that it regularly receives reports from state governments on sexual predators and takes down such profiles within 72 hours.[191] This practice, according to Facebook's chief privacy officer, is a welcome one: "[Facebook] want[s] to be a good partner to the states in attempting to address this societal problem . . . We've worked with them for quite some time now, and we look forward to continuing our fruitful partnership."[192] This partnership has even led Facebook, MySpace, and Yahoo to lobby for state legislation that requires sexual offenders to register their names and e-mail addresses with the state so they can block such criminals from registering.[193]

---

[189] Admittedly, this would not be a costless measure for websites, as they would have to employ administrators to clean up websites and manage problems. This, however, would presumably remain less expensive than hiring liaisons to manage regular police incursion and government surveillance on their servers.

[190] Juan Carlos Perez, *N.Y. E-Safety Bill Gets Facebook, Myspace Support*, ABC NEWS, Jan. 30, 2008, http://abcnews.go.com/Technology/PCWorld/story?id=4214843 ("The attorneys general [of various states] have often criticized Facebook, MySpace and other sites for, in their view, not doing enough to protect minors, but the two sides have recently seemed to get on better terms and have rolled out several joint security initiatives, partnerships and agreements.").

[191] Brad Stone, *Facebook Hears Accusations About Sexual Predators*, N.Y. TIMES, July 30, 2007, at C1.

[192] *Id.*

[193] Perez, *supra* note 187.

1. THE GOVERNMENT SHOULD ENLIST WEBSITE ADMINISTRATORS—NOT FIGHT THEM.

Unfortunately, many states forged these partnerships in the crucible of adversary court tactics. Instead of seeking cooperation, states like New York, Connecticut, and North Carolina initially issued subpoenas against social networking sites,[194] forcing sites like Facebook and MySpace to engage in costly negotiations with governments as adversaries. This antagonism is wrong-headed because it forces both the websites and the states to incur unnecessary legal and court costs that could otherwise be spent on crime-fighting. Through these litigation expenses, states essentially taxed Facebook and MySpace for the very innovative social features they employed to curb deviant behavior.

Although New York has wisely retreated from this adversarial posture,[195] others continue to vary in their approaches. At present, no state offers subsidies or rewards for website communities that foster social norms or cooperate with authorities; sites like Facebook and MySpace incur these costs as a price of doing business on the Internet.

2. THE FEDERAL GOVERNMENT SHOULD ENCOURAGE SOCIAL NORM GROWTH ON WEBSITES AND GOVERNMENT-WEBSITE COOPERATION.

Since the fifty states are balkanized in their cooperation efforts, the federal government must step in. Through legislation, Congress should refocus its finite resources away from invasive FBI broken windows tactics and towards techniques that encourage Internet

---

[194] *See* Anne Barnard, *New York Investigating Facebook's Safety Rules*, N.Y. TIMES, Sept. 25, 2007, at B3 ("Yesterday, [the New York] attorney general's office issued a subpoena to the company requesting documents related to the security that Facebook promises to its 42 million users and how it resolves complaints."); Jenna Wortham, *MySpace Turns Over 90,000 Names of Registered Sex Offenders*, N.Y. TIMES, Feb. 4, 2009, at B4 ("MySpace provided two state attorneys general the names of 90,000 registered sex offenders it had banned from its site in response to a subpoena.").

[195] Anne Barnard, *Facebook Agrees to More Safeguards*, N.Y. TIMES, Oct. 17, 2007, http://www.nytimes.com/2007/10/17/nyregion/17facebook.html; Karen Freifeld, *New York Settles Facebook Probe; MySpace Subpoenaed*, BLOOMBERG NEWS, Oct. 16, 2007, http://www.bloomberg.com/apps/news?pid=20601103&sid=aX2IgZbusIhE&refer=us# .

self-policing. Instead of penalizing social networks, Congress should consider rewarding innovations, and perhaps even subsidize sites that facilitate social norms on websites. Since sites like eBay and Facebook have already proven that social norms *are* possible on the Internet and can efficiently discourage Internet deviance through real name registration and sign-in requirements, Congress can encourage other website administrators to employ similar reputation and transparency systems through tax incentives and other means.

Facebook and eBay do not necessarily construct social norm mechanisms because it is the right thing to do; these sites employ them because it is profitable; social networking is inherent in their business models.[196] Congress can facilitate this profitability and protect the social norms that are proliferating in cyberspace. Most importantly, Congress could tether these subsidies to requirements that these sites continue to (1) facilitate social norms and (2) cooperate with law enforcement.

To protect the efficacy of such market incentives, Congress should also grant immunity to social norms websites that cooperate "in good faith" with the government. The "fruitful" partnership between the government and social norms websites can still bear more fruit, but only if local governments stop pitting themselves against their potential partners. Through a national policy that encourages cooperation, governments can ensure social norms policing on existing websites like eBay and Facebook, encourage other websites to employ similar techniques, and embrace a new crime-fighting partnership that will inhibit Internet crime without inhibiting disrespect for the law.

CONCLUSION

Law-abiding behavior, like any behavior, is a complex and interdependent social arrangement. It requires constant support and reinforcement, and in anonymous "loose-knit" communities like the city and the Internet, this support seems to be lacking. But on the Internet, some websites have already facilitated law-abiding behavior through voluntary registrations, visitor-to-

---

[196] *See, e.g.*, Stone, *supra* note 178.

visitor communication, and reputation systems. Through these techniques, certain websites have shrunk the Internet from a far-flung urban feel to a close-knit "village" capable of fostering social norms.

In order to fight crime, law enforcement should avoid costly and intrusive tactics that might disrupt these budding communities. Such tactics did not work in the city context, and they will not work on the Internet. As in the city, these tactics threaten to counteract the development of productive social norms with a dangerous disrespect for the law. Instead, law enforcement should encourage technological norm innovation, forge partnerships with website administrators, and use their finite resources to amplify social norms wherever possible. Such norm-minded policing is a costless and effective means of curbing deviant behavior, and more importantly, harnesses the Internet's boundless social energy and unyielding versatility towards the creation of social norms.

This is a unique opportunity. Policymakers can potentially avoid the crime-fighting mistakes of the city's past with the dynamic understanding of the Internet's future. And they can do it today, if they would only consider the simple question:

What would people think?