Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model [*]

Susan W. Brenner
NCR Distinguished Professor of Law & Technology
University of Dayton School of Law
Dayton, Ohio USA 45469-2772
Email: **susanwbrenner@yahoo.com**

Abstract: It is apparent that law enforcement, alone, cannot effectively combat cybercrime. One possible way to improve national responses to cybercrime is to incorporate cooperation with the private sector into the effort. But what are the limits and the legality of bringing private actors into the criminal justice process? This paper analyzes two ways in which the current law enforcement model could be modified to incorporate limited civilian participation in cybercrime investigation and prosecution processes.

1. Introduction

As I have explained elsewhere, the model of law enforcement we currently rely upon is not effective in dealing with cybercrime, at least, is not as effective as it needs to be to control the incidence of cybercrime (Brenner, 2004).

The current model is not effective because, reasonably enough, it was developed to deal with real-world crime. As a result, it incorporates (i) certain assumptions about crime and (ii) correlative assumptions about how law enforcement reacts to completed crimes in a manner that sustains the level of deterrence needed to keep crime under control. The model is not effective against cybercrime because the assumptions it makes about crime do not hold for cybercrime: Unlike crime, cybercrime is routinely transborder/transnational in nature, which means there is usually not a single, localized crime scene that becomes the focus of an investigation; and because it is automated, cybercrime is routinely committed on a scale vastly exceeding the scale on which it is possible to commit crimes. Singly and in combination, these factors create challenges for law enforcement's investigatory procedures and resources. (Brenner, 2004)

For these and other reasons, the current law enforcement model – which makes the process of reacting to crimes (or cybercrimes) the exclusive province of a cadre of government-sponsored, professional law enforcement agents – is not, and will never be, adequate to keep cybercrime and related evils such as cyberterrorism within acceptable bounds. Indeed, the problems we see with the current model will only be exacerbated as computer technology migrates from the "boxes" we currently use and embed itself into our environments and, perhaps, into ourselves.

In the early nineteenth century, Sir Robert Peel invented a new approach to crime control because the strategies being used were simply not effective. He gave us the model we currently use, which is still effective for traditional crime.(Brenner 2004) We, though, face challenges Sir Robert could not have imagined, challenges that erode the efficacy of the model he created. We must, therefore, devise a new approach for the new problems we face.

Since the current model is adequate for real-world crime, and since much of the crime societies confront is still real-world crime, we should not discard the current model. The prudent course, instead, is to modify the current model in a way that enhances its ability to react effectively to cybercrime and related evils. This paper analyzes how we might go about doing this. It is very much on the order of a speculation – an effort to parse the conceptual and legal issues that would arise from what seem to be the most viable options for modifying the current model.

The sections below undertake this process. They focus on two fundamental modifications of the current model, both of which entail expanding the pool of citizens who participate in the reacting-to-cybercrime process and changing how they participate. The first modification incorporates civilian participation and civilian

[*] A version of this paper was published in Kierkegaard, S. (2006) Business Law and Technology Vol. 1 and presented in the 2006 IBLT Conference , Denmark.

resources into this process; this approach in a sense "deputizes" the civilian participants, because their participation becomes a formal component of the process. The other modification tolerates independent, idiosyncratic civilian efforts to react to cybercrime; this approach represents the legitimization of vigilante action, at least in the cyberworld.

Before I proceed with the analysis, I should note that my focus in this paper is very different from the focus I have brought to bear on this issue in prior papers. I have argued, elsewhere, for using criminal liability to encourage civilians – individual and corporate civilians alike – to prevent cybercrime. My focus in those papers was on using criminal liability to effect a change in culture – moving us from a culture in which we regard cybercrime as the sole province of law enforcement to one in which we assume a measure of responsibility for protecting ourselves from online miscreants. Such a shift in culture, of course, also represents a modification to the current law enforcement model.

I see that modification, though, as a much more informal process, even though it is instituted via the selective use of the criminal sanction. While civilians play a de facto role in the current law enforcement model under that proposed modification, they do so while remaining outside the formal law enforcement structure. Under that modification, they function as ad hoc adjuncts to professional law enforcement efforts. They have no official status, and they play no role in the formal law enforcement process. Their only role – their only contribution – is to reduce the incidence of cybercrime by taking certain prophylactic measures to secure their activities and their computers. Their participation is, in a sense, passive; they try to block cybercrime, rather than investigate it.

I see the modifications I explore in the sections below as a more radical step, since both actively involve civilians in the process of reacting to completed cybercrimes. In these modifications civilians do not function merely as adjuncts to professional law enforcement officers; instead, they effectively step into law enforcement's shoes and actively participate in the process of pursuing cybercriminals. The modifications we examine below are therefore structural – rather than cultural –modifications. As such, they raise difficult questions about the proper relationship between civilians and their government, as personified by the officers charged with enforcing the criminal laws. We will return to this issue at the end of the paper.

We begin by analyzing the permissibility and practicality of incorporating formalized civilian participation into the reacting-to-cybercrime process. We will then do the same for the vigilante modification.

1.1 Formalized Civilian Participation

This analysis involves two distinct dichotomies. The first goes to *how* civilians participate in the reacting-to-cybercrime process – the role(s) they play in the process. Our approach to law enforcement encompasses two phases: (i) investigatory, in which agents of the state identify and apprehend offenders; and (ii) prosecutorial, in which the offenders are tried and, optimally, convicted and sanctioned for their transgressions. Logically, civilians can participate at either or both levels; that is, they can participate in the process of investigating cybercrime and/or in the process of prosecuting cybercrime.

We explore both options in the sections below. But each option also presents a secondary dichotomy: What are the conceptual issues involved in implementing this version of the formalized civilian participation modification? And what are the practical issues involved in doing so? We also address these issues below.

Our analysis of the formalized civilian participation modification follows the first dichotomy: The initial section below examines the conceptual and practical issues involved in incorporating formalized civilian participation into the process of investigating cybercrime. The next section examines the conceptual and practical issues involved in incorporating formalized civilian participation in to the process of prosecuting cybercrime.

1.2 Investigating Cybercrime

Unlike prosecution, which has (at least in the United States) included a measure of civilian participation, the investigation of crime has been exclusively reserved for law enforcement officers since the model developed by Sir Robert Peel became entrenched in societies toward the end of the nineteenth century Brenner 2004). Civilians' only roles in the model devised by Sir Robert are to act as (i) the complainant, whose information often initiates an investigation and (ii) a witness if and when the matter goes to trial.

This approach is not historically inevitable; civilians played an active role in the investigation of crime prior to Sir Robert's innovations. Citizens of most pre-nineteenth century societies would find our limiting

investigatory efforts to professionalized officers peculiar, as their societies relied upon a mix of public and private efforts.

We cannot, however, simply go backwards, even in the face of evidence that our current approach is not satisfactory. When the prospect of incorporating active civilian participation into the battle against cybercrime has been raised – and it has come up in several, somewhat limited contexts, as we see in a moment – it has been met with some resistance, resistance based on issues that may or may not be serious and that may or may not be merely the product of our discomfort with deviating from the law enforcement model to which we are accustomed.

1.3 Individual versus Corporate Participation

Before we analyze the arguments for and against active civilian participation in the investigatory process, we need to parse out the forms that participation might take. Overall, the most substantial (and therefore most useful) participation would come from corporate civilians, because they generally have the most resources to draw upon. Basically, a corporation can participate in two, non-exclusive ways: It can supplement the non-personnel resources available to law enforcement by contributing materiél – hardware, software and other items needed in the investigatory process – to the officers charged with pursuing cybercriminals. This has been, and is being, done in the United States and elsewhere. The other way a corporation can contribute is by assigning its own personnel to work with law enforcement in the investigatory process. This, too, has been done, at least in the United States.

Individuals could participate in the investigatory process, but their participation is more problematic, for several reasons. Overall, individuals are less likely to be able to donate substantial, useful resources to enhance the resources already available to law enforcement officers. There will be some exceptions, but any systemic modification of the current model must be based on general principles and enunciate general standards authorizing civilian participation in the investigatory process. We will therefore assume that individual civilians, as a class, cannot contribute resources the substantiality of which would markedly enhance the effectiveness of law enforcement officers' ability to investigate cybercrime.

The inferentially limited resources that are likely to be available from individuals are one reason for not including individual civilian participation in the modification we are analyzing. Professionalism may be another reason to exclude individuals from this process: If we were to allow corporate civilians to assign their personnel to assist law enforcement in cybercrime investigations, we would presumptively be enhancing the effectiveness of professional law enforcement personnel by supplementing their efforts with those of other professionals. The civilians' professionalism would, concededly, be in areas other than law enforcement, but they would have useful, specialized expertise and would participate in the investigatory process as professionals, not as victims of the cybercrime being investigated. Like the officers they would assist, the civilians assigned by their corporate employer would participate in a disinterested, purely professional capacity.

Their corporate employer would no doubt be a current, past and/or prospective future victim of cybercrime, but that should not significantly affect the professionalism with which they play their respective roles in the investigatory process. The complex organizational structure common to modern corporations should serve to insulate these technically-adept experts from any residual rancor or other affective artifacts that might derive from the corporation's own victimization. And emotional reactions, if any, are highly unlikely to prompt civilian organizations' participation in the investigatory process; corporations are much more likely to participate because they understand that a globally effective official reaction is their best guarantee of continued security.

This brings us back to the rather problematic issue of allowing individual civilians to participate in the investigatory process and to the specific issue of professionalism. Individual civilians (i) may be professional but (ii) may not be professional. While there are many, many extremely professional technical experts of varying types in every country, they are definitely the exception. The appropriate default assumption for individual civilian participation is, therefore, that we would be allowing non-professionals to participate in the cybercrime investigatory process. This assumption then generates two questions: What are the benefits of allowing individual civilian participation in this process? What are the disadvantages, the downsides, of allowing this?

The benefits, if any, seem to be minimal. Centuries ago, participation in the law enforcement process by lay individual civilians supplemented the manpower – the base physical resources – available to track down and apprehend fleeing criminals. Since cybercrime is virtual, not physical, crime, adding additional manpower (personpower) would in no way increase the effectiveness of the law enforcement effort.

Indeed -moving to the second question - it seems more likely that introducing the participation of lay individuals who have no useful computer or related expertise would impede the efforts of law enforcement personnel, as they would have to devote some time and resources to dealing with these people. Another disadvantage, another downside, is that these individuals are likely to be motivated to participate in the process because they have been the victims of cybercrime. The fact of their victimization would inevitably import an emotional element into their participation that is inconsistent with, and antithetical to, the professionalism we must maintain in the reacting-to-cybercrime process.

It seems, then, that the best approach would be to limit civilian participation in the process of investigating cybercrime to corporate civilians. Individual civilians could still contribute to the process by securing their computer systems and otherwise preventing cybercrime. They are also the focus of the vigilante modification, which we analyze later in this paper.

1.4 Corporate Participation in the Investigatory Process

We will first identify how corporate civilians can participate in the reacting-to-cybercrime process, and then analyze the conceptual issues such participation raises. As noted above, there are two ways in which corporate civilians can participate in this process: They can provide law enforcement officers with relevant resources – hardware, software, other useful items and services – which supplement those already available. They can also participate more directly, by assigning members of their own staff to work with law enforcement officers on the reacting-to-cybercrime process. We will analyze

In the United States, corporations have been donating hardware, software and other items to cybercrime-focused investigative units for years. Perhaps the most dramatic example of this occurred after the New York Secret Service Field Office was destroyed on September 11, 2001, when World Trade Center 7 collapsed. The office, which then had the largest, most professional cybercrime investigative unit in the United States, lost everything: all the stored evidence, all of the office's computer equipment and its network. The New York Field Office's computer unit was, however, up and running forty-eight hours later, thanks to the effort and donations of 200 corporations and several universities.

The restoration of the New York Field Office's computers and network is a dramatic example of something that has become routine in many agencies around the United States. Microsoft, for example, funded a $250,000 computer crime lab that is being used to train cybercrime investigators. Gateway donated a mobile wireless computer lab for the same purpose. And in Austin a number of high-profile corporations joined together and created a foundation that funds the resource and other needs of the Austin High-Tech Crime Unit. These are but a few examples of activity that is occurring elsewhere in the United States, but remains an ad hoc, localized phenomenon.

One reason why this practice remains an ad hoc localized phenomenon may be the lingering uncertainty, even discomfort that U.S. officers, agencies and citizens feel about having police rely on donations from private sources. The U.S. Department of Justice's Computer Crime and Intellectual Property Section sought to address these concerns in a 2003 report. (Zentner & Klumb, 2003)

The report begins by distinguishing assistance from gifts (Zentner & Klumb, 2003). It notes that law enforcement has "traditionally relied upon assistance from victims and witnesses" and that assistance is generally unproblematic. It describes assistance as testifying in court, providing physical evidence, consulting with law enforcement to help analyze evidence or facts and similar activities. The essential defining characteristic of "assistance" seems to be that it comes either from the victim of the crime, witnesses to the crime or experts who work with law enforcement on a specific crime or crimes. The report then identifies the circumstances under which "aid or cooperation" will be considered a "gift," rather than "assistance:" A contribution of cash by anyone – even the victim of the crime being investigated -- will always be considered a gift. (Zentner & Klumb, 2003) Other "aid or cooperation" from a victim will be considered a "gift" if it is not given "in connection with and limited to a specific case . . . involving that victim". And any aid, cooperation or funds from a disinterested third party constitutes a "gift," not "assistance". (Zentner & Klumb, 2003)

The report specifically lists the following as examples of "gifts" from unrelated third parties: conducting a forensic analysis of evidence; providing space or equipment; providing training for agents or prosecutors.(Zentner & Klumb,2003) In an earlier section, the report explains that it is "assistance" for a company to provide law enforcement officers with computers and software to be used in investigating crimes against the company, but becomes a "gift" if the company lets the government "use the computers for unrelated investigations and prosecutions". (Zentner & Klumb, 2003) The report then analyzes the extent to which

applicable federal statutes, regulations and ethical standards permit federal agencies to accept "assistance" and "gifts."

The latter are far more problematic because, as the report notes, they give rise to concerns about the fairness and impartiality of the law enforcement process. (Zentner & Klumb, 2003) Indeed, some characterize non-victim, nonspecific corporate donations of computer resources and personnel to law enforcement agencies as "buying justice." Others have defended it, essentially, as a necessary evil.

As I noted earlier, it is necessary, but whether it is inevitably an "evil" is more problematic. If corporate donations necessarily result in law enforcement's losing its independence and becoming the agent of private donors, then allowing such donations is certainly an evil and we must rethink this aspect of the modification we are exploring. It may be, however, that the perception – or the reality – that law enforcement tends to lose a measure of its professional independence when it relies, even in part, on outside resources, is merely an artifact of our essential inexperience with this strategy.

The usually-articulated criticisms of the strategy focus on the notion cited above: the premise that the corporate donors are "buying justice" for themselves, at the neglect of other, equally-deserving victims. This is certainly an empirical possibility, and it has no doubt happened in the past. The fault, though, may lie not with the strategy but with the informal way in which it has been implemented. If companies donate directly to law enforcement agencies, and if the agencies come to depend on those donations, then the agency personnel may become . . . malleable, open to being influenced by the donor's articulated priorities and preferences.

Donations can, though, be structured in a way that allows law enforcement to preserve its independence. The foundation that funds the efforts of the Austin High-Tech Crime Unit is a good example. The foundation is funded by a consortium of private corporations that want cybercrime enforcement to be pursued diligently and effectively by local officers, but it is independent of the funding entities and therefore acts as a mediating force between the donors and the agencies that benefit from the donors' generosity. This approach could be used to allow law enforcement agencies to gain the additional resources they require to improve their efficacy in reacting to cybercrime without surrendering any of their autonomy.

Before we turn to prosecution -- the other way civilians can participate in the reacting-to-cybercrime process – we need to at least briefly consider two residual issues that can arise from allowing corporate civilians to participate in this process.

The first issue goes not to the subversion of investigatory independence but to compromised confidentiality and conflicts of interest arising from the active participation of corporate employees in the investigation process. Assume Company A has assigned five of its computer security experts to work with the local Metropolitan Computer Crime Task Force (MCCTF) for a period of six months. For six months, the employees spend their working hours exclusively at the MCCTF, helping the law enforcement officers who staff the Task Force with cybercrime investigations. Now assume that Company B – a competitor of Company A's – is the victim of a large-scale, complex cybercrime attack. Is it permissible for the on-leave Company A employees to assist with the investigation of this attack? If they do participate in the investigation, it is reasonable to assume that they will have access to information, confidential information that Company A could use to compete more effectively with Company B. Does this disqualify them from assisting with the investigation? If so, does this mean that the contributions of corporations must be limited to equipment and other non-personnel resources? Or could the problem be resolved by having the on-leave Company A employees sign a confidentiality agreement that encompasses all their activity while they are assigned to the MCCTF? Would their execution of such an agreement be sufficient to allay the fears of companies that might be hesitant to have the agents of rival corporations given any access to their computer systems?

The other issue would be particularly important in the United States – where the Fourth Amendment constrains law enforcement activities – but might be less important in countries where the restrictions on law enforcement investigations are less stringent. In the United States, the Fourth Amendment applies only to the activities of police and other investigatory agents of the government; it has no application to private citizens who may decide to assist law enforcement by, say, collecting evidence and bringing it to police. The Fourth Amendment, however, does apply when private citizens have been recruited to work with law enforcement agents in the investigatory process; at that point, the citizens become agents of the state, and are therefore bound by the restrictions the Fourth Amendment imposes on all state investigatory activities. This has several implications for the prospect of allowing corporate civilians to assign their employees to work with law enforcement on cybercrime investigations.

The most obvious, and least problematic, implication is that the employees would be considered agents of the state bound by the Fourth Amendment as long as they were assisting law enforcement with an investigation.

So in the hypothetical given above, the on-leave Company A employees would be agents of the state during the six months they are assigned to work with the MCCTF. During that time they, like the officers they would be assisting, would have to obtain search warrants and otherwise comply with Fourth Amendment requirements. The more difficult implication arises when the collaboration between corporate employees and law enforcement is not as structured, as contained, as it is in the hypothetical given above.

What if instead of assigning employees to spend six-month periods working exclusively with the MCCTF, Company A simply has its employees assist the MCCTF whenever the agency needs help with a cybercrime investigation? This is no doubt the more likely scenario for the type of corporate participation we are analyzing, since it may be difficult or even impossible for a company simply to re-assign one, two, three or more of its computer security people to work with law enforcement for an extended period of time. The collaboration is much more likely to be situational, and sporadic, and that will make the state-agent analysis much more complex. The government would argue that the employees were agents of the state subject to Fourth Amendment requirements only when they were actually assisting with a cybercrime investigation at the behest of law enforcement. Defendants moving to suppress evidence (and also, perhaps, civil liberties advocates) would claim that because of the continuing nature of the collaboration, the employees of Company A (and Company B and Company C and any other company involved in such an arrangement) had become permanent agents of the state and so were always subject to Fourth Amendment restrictions, even when they investigated attacks on their own employer. Courts would have to decide which argument prevails, but even if they side with the defense/civil liberties advocates, this should not doom the strategy we have been exploring. It would simply mean that corporate employees would have to abide by the requirements of the Fourth Amendment, even in conducting purely internal investigations.

Before I turn to the issue of allowing civilian participation in the prosecution of cybercrime, I want to note my understanding (or misunderstanding) of how the scenario I outline in the paragraph immediately above would play out in other countries, notably in many European countries. It is my understanding – and here I am probably greatly oversimplifying these matters – that European Union privacy laws tend to impose more restrictions on corporations, while the opposite is certainly true in the United States. The situation in the United States creates the dilemma outlined above, in which corporations become subject to more investigatory (privacy) restrictions if they collaborate closely with law enforcement agencies. I wonder if the opposite would be true under European Union law. Would corporations be subject to fewer investigatory (privacy) restrictions if they were to enter into a sustained collaboration with law enforcement for the purpose of investigating cybercrime? Or would it have the opposite effect – would law enforcement agencies become subject to the European Union restrictions that apply to corporations as the result of entering in to such collaboration?

I cannot answer those questions. Indeed, I may be incorrect in posing them. My point is simply that modifying our law enforcement model to import a substantial level of collaboration between corporate civilians and law enforcement agents will require us to reconcile existing laws governing privacy and law enforcement investigations with the fused efforts such collaboration will produce.

1.5 Prosecuting Cybercrime

The need to supplement the resources and personnel available to investigate cybercrime is the most pressing problem with the current law enforcement model, but it is appropriate to consider the related issue of allowing civilians to bring prosecutions for cybercrime. In this section, I briefly trace the history of private prosecution in the Anglo-American tradition and then analyze whether permitting privately-initiated prosecutions of cybercrime would be a useful, justifiable modification to our current approach to crime.

Private prosecution has a long history in Anglo-American law. They originated in England at a time when "the legal system primarily relied upon the victim or the victim's relatives to bring a criminal to justice." In the latter part of the nineteenth century, British authorities made an effort to abolish private prosecutions because reformers such as Jeremy Bentham and Sir Robert Peel argued that the system produced certain evils. One of the evils most often identified with private prosecutions was the premise that they often led to prosecutions that were instituted out of personal animosity or a desire for revenge, rather than a desire for justice. The British government eventually established the Office of Director of Public Prosecutions in an effort to eliminate private prosecutions, but British citizens still have the right to initiate criminal proceedings.

Colonists brought the system of private prosecution to America, where it survived until the end of the nineteenth century. As in England, the system came under criticism from courts and others who felt it distorted the concept of prosecutions as the instrument of justice. In 1888, the Wisconsin Supreme Court explained why

private prosecutions are objectionable: "The prosecutor has a duty to present evidence favorable to the defendant. . . . [C]riminal cases are not likely to be so presented if the prosecution is . . . conducted by the paid attorneys of parties who from passion, prejudice, or even an honest belief in the guilt of the accused, are desirous of procuring his conviction."

The alternative system of public prosecution began to appear even before the American Revolution. The creation of the office of public prosecutor seems to have been the result of European influence in the colonies, most notably from the French and the Dutch. Public prosecution became increasingly common in the nineteenth century, and has effectively supplanted private prosecution in the United States. But while private prosecution has fallen into disfavor, there is no legal authority establishing that it is unconstitutional or otherwise fundamentally unacceptable. Private prosecutions crop up occasionally, and though courts sometimes express reservations about the practice, they are upheld. (Cronan, 2001)

Private prosecutions do raise concerns about the motivations responsible for the pursuit of particular charges, but the actual conduct of the prosecution itself should be less problematic. Courts can apply constitutional and evidentiary principles to ensure fairness in private prosecutions, just as they do with publicly-initiated prosecutions. This is not to say that – at least from the perspective of an American lawyer – private prosecutions should become the norm. Used judiciously, they can serve a useful purpose in systems that otherwise rely upon publicly-initiated prosecutions. As some have noted, they allow the victims of crime (or cybercrime) to seek justice when a public prosecutor has decided not to pursue a case or is delaying the decision on whether or not to prosecute. (Sidman, 1975) In this regard, they provide additional protection for crime victims and, inferentially, anyway, enhance the deterrent effect associated with the increased possibility that one will be prosecuted for particular offenses. (Sidman, 1975)

Private prosecutions could be a way to increase the likelihood that cybercriminals will be prosecuted and convicted and thereby increase the disincentives associated with the commission of cybercrime. In the United States, anyway, anecdotal evidence shows that many prosecutors – especially at the state and local level – are disinclined to take on cybercrime cases, for several reasons. (Brenner & Schwerha, 2002) One reason is that they are not familiar with the legal issues involved; another is that the case may involve complex jurisdictional issues with which they are unfamiliar. Another is the case will probably raise issues involving the admissibility and reliability of digital evidence, and most state and local prosecutors are not technologically-educated and so do not feel competent to take on these issues.

Yet another reason is the issue of resources, again: Public prosecutor's offices at the state and local levels operate on limited budgets; due to the technical and/or jurisdictional complexity of cybercrime cases, one cybercrime prosecution can seriously erode the resources available to that office. (Brenner & Schwerha, 2002) This means that, at best, state and local prosecutors will only be able to take a few -- a very few -- cybercrime cases to trial. (Brenner & Schwerha, 2002) And while prosecutors in the U.S. federal system have more resources at their disposal, they, too, must be very selective in the cases they choose to take to trial. Also, federal prosecutors make up a very small percentage of the prosecutors in the United States; the default model is for prosecutions to be initiated at the state and local level. (Brenner & Schwerha, 2002)

The result is that many, many cybercrime cases go unprosecuted. After I spoke at a cybercrime training program held in one of the largest cities in the United States, I had the opportunity to chat with a senior detective in the local police force, a man who handles only economic crimes. He told me he "catches the same people over and over" when it comes to cybercrimes, because the local prosecutor does not want to pursue them, for any or all of the reasons outlined above. The result is that no charges are brought and the perpetrators can re-offend with a reasonable assumption of impunity.

Allowing private prosecution of cybercrime – even of some types of cybercrime – could help to alleviate the difficulties U.S. prosecutors, anyway, are experiencing in this area. Allowing private prosecutions of cybercrime would give cybercrime victims who are otherwise left without the hope of justice an alternative; they could initiate their own prosecutions, subject to guidelines that would have to be established to control vindictive prosecutions and prevent the judicial system from being overwhelmed with problematic private prosecutions.

Articulating the nature of those guidelines is outside the scope and ambitions of my effort here. They could institute a practice many federal prosecutors are currently following on an ad hoc basis: They could limit the institution of a private prosecution to instances in which the loss was "more than trivial," either in terms of financial losses or in terms of reputational, emotional or other legally-cognizable harms. They could limit the institution of private prosecutions to certain types of cybercrime; no one, presumably, would want to see cybercrimes involving terrorism, property destruction, homicide or the infliction of physical injury prosecuted by laypeople.

Another way to guard against frivolous or vindictive prosecutions – and ensure prosecutions are likely to be brought by those who can summon the resources to pursue them effectively – would be to limit the institution of private cybercrime prosecutions to corporate or other professional victims (law firms, physicians, etc.). It seems reasonable to assume that corporate entities and professionals are less likely to pursue criminal charges out of malice or a misguided sense of justice than are average citizens. This is not to say that average citizens categorically could not base their decision to prosecute on the same type of rational calculus we are inferentially imputing to corporations and professionals. It is to say that the American experience with pro se litigation teaches us that citizen-initiated litigation is often more the product of emotion than of reason. (Henderson, 2003)

Our experience with pro se litigation also teaches us that civil suits brought by laypeople tend to be particularly burdensome on courts and on opposing counsel both because the lay litigants are acting out of emotion and because they do not understand the procedural rules governing litigation. (Champion, 2005) While the U.S. legal system is willing to tolerate these burdens to give citizens who cannot obtain private counsel the opportunity to seek civil justice, different considerations come into play when criminal charges are involved. Even courts that accept private prosecution have held that it is not an acceptable option when a conviction can result in imprisonment. (Martineau, 2002)

Limiting private cybercrime prosecution to corporations and professionals would alleviate, if not eliminate, concerns about vindictive prosecution. It would also serve to reduce the risk that the private prosecutor would not be capable of mastering the rules governing the litigation, since it is reasonable to infer that corporate and professional cybercrime victims would retain attorneys to act for them in bringing a prosecution.

The other advantage of limiting private cybercrime prosecution to corporate and professional civilians is that they are more likely to have the resources needed to pursue a prosecution effectively and obtain a conviction, when one is warranted. As I noted earlier, cybercrime cases tend to be resource-intensive prosecutions, requiring computer forensic and other experts to analyze evidence and testify at trial. Optimally, they can also require the services of litigation support personnel who can develop simulations and other visual aids that help the jurors understand the nature of the crime and how it was carried out.

Depending on the constraints imposed by a legal system, it seems that private prosecution by corporate and professional victims could be a useful way to increase the number of prosecutions and convictions and thereby raise the stakes for cybercriminals.

2. Legalized Vigilantism

This oxymoron is a logical but, I submit, an unacceptable way to bring increased resources and personnel into the cybercrime investigation process. To understand why I believe legalizing vigilantism is unacceptable, I need to define vigilantism and distinguish it from the first modification we examines, the notion of allowing civilians to participate in the process of investigating cybercrimes.

In popular culture, vigilantes are often associated with the American West, where citizen groups emerged to fill the vacuum resulting from a total lack of law enforcement personnel. (Sklansky, 1999) Definitions of vigilante vary, but they all have one thing in common: A vigilante is someone who assumes the responsibility of investigating and/or punishing those who commit crimes because the formal mechanism of law enforcement is absent or ineffective. (Burrows, 1976)

Cyberspace is an obvious venue for the emergence of vigilantism. As I noted earlier cyberspace presents many challenges for law enforcement, the result being that online law enforcement is at least ineffective. Not surprisingly, therefore, vigilantes are emerging online.

Online vigilantism takes various forms. Some groups – like Artists against 419 (AA419) – function as traditional vigilantes in that they directly target cybercriminals. (Wikipedia, 2006) AA419 members use denial of service attacks and other extralegal devices to shut down websites used by 419 scammers. (Wikipedia 2006) Like Old West vigilantes, the AA419 vigilantes take the law entirely into their own hands, acting as prosecutor, judge, jury and executioner.

Online vigilantism of the type practiced by AA419 members is subject to the same objections that have made real-world vigilantism illegal. One is the unacceptable risk of error. Because vigilantes act autonomously, on the basis of personal knowledge unfiltered and unmediated by the participation of others, they are likely to make mistakes in identifying a perpetrator or even in concluding that a crime has bee committed. (Clark 2001). Formal law enforcement and adjudicatory systems also make mistakes, but their procedures tend to minimize mistakes and provide a mechanism for correcting them. Another objection to the AA419-type of online vigilantism is the risk of injury resulting from their unauthorized use of force. The risk of excessive force has

traditionally been a factor militating against societies' acceptance of vigilantism. (Hine, 1998) While the AA419 vigilantes do not use physical force, they employ virtual force to similar, if not equal, effect; online or offline, societies simply cannot tolerate the unsanctioned use of retributive force by civilians.

Another, novel type of vigilantism has emerged online. Probably the best-known example of this kind of vigilantism is Perverted Justice, the group that works with law enforcement to identify and bring online pedophiles to justice. (Perverted Justice, 2006) Perverted Justice is famous (or infamous) because it teamed up with NBC television to broadcast pedophile "stings." (MSNBC, 2006) Perverted Justice members go into chat rooms where they pretend to be underage boys and girls. When approached by men seeking sex, they play along and eventually agree to meet the man they are chatting with at a place set up by Perverted Justice and NBC producers. When the men arrive, they are videotaped making incriminating statements and then arrested by police who cooperate in the process; portions of the tapes are then broadcast. (MSNBC, 2006)

Perverted Justice vigilantes work with law enforcement to apprehend pedophiles, rather than taking justice entirely into their own hands. Their efforts are analogous to the civilian participation model outlined above insofar as they work with law enforcement, but they deviate from that model in at least one, critical respect. Perverted Justice members initiate the investigations and completely control the process of bringing suspects to law enforcement; aside from anything else, this imports a substantial risk into the process, a risk both of targeting individuals unjustifiably and of committing procedural errors that may result in prosecutions' being quashed and/or evidence suppressed. If we are to allow civilian participation in the cybercrime investigation process, that participation must always be subject to and constrained by law enforcement authority. Otherwise, we are merely sanctioning a variant of the vigilante activity that has historically been prohibited.

3. Conclusion

As the Department of Justice study noted, "the monopolization of policing by government is an aberration. It is only in the last one to two hundred years that policing has been effectively monopolized by government". (Bayley & Shearing, 2000) The monopolization model invented by Sir Robert Peal in the nineteenth century was an appropriate response to a particular situation – the increasing inefficacy of the existing model in the face of urbanized crime.

We face a very different crisis – decentralized, nonlocalized cybercrime committed on a hitherto impossible scale. Like Sir Robert, we must not be afraid to innovate, to experiment with new solutions. Though it may seem an impermissible aberration from the concept of policing to which we are accustomed, incorporating civilian participation into law enforcement on a limited, controlled basis is actually a return to an older approach, one that antedated professional policing.

Professional policing works well for real-world crime, and should remain the dominant model in that arena. Professional policing does not, and probably cannot, work as satisfactorily for cybercrime because of the factors I noted at the beginning of this paper. We might be able to make professional policing work satisfactorily for cybercrime if we were able to devote massive resources to increasing professional policing's staff and resources, but that will almost certainly not happen, for various reasons. The strategy I outline in this article is a compromise based on the premise that we need innovative solutions for innovative crime.

REFERENCES

1. Bayley, David H. & Shearing, Clifford D. (2000). The New Structure of Policing. Washington, D.C.: U.S. Department of Justice.
2. Bessler, John D. (1994). *The Public Interest and the Unconstitutionality of Private Prosecutors.* 47 Arkansas Law Review 511.
3. Biemel v. State, 37 N.W. 244 (Wisconsin Supreme Court 1888).
4. Brenner, Susan W. (2004). *Toward A Criminal Law for Cyberspace: Distributed Security.* 10 Boston University Journal of Science & Technology Law 1.
5. Brenner, Susan W. & Joseph J. Schwerha IV (2002). *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime.* 20 John Marshall Journal of Computer and Information Law 347.
6. Burrows, William E. (1976). Vigilante! New York: Harcourt Brace Jovanovich.
7. Champion, Brian L. (2005). *Defending Against A Pro Se Plaintiff.* 20 Maine Bar Journal 236.
8. Clark, Walter Van Tilburg (2001). The Ox-Bow Incident. New York: Random House.

9. Cronan ex rel. State v. Cronan, 774 A.2d 866 (Rhode Island Supreme Court 2001).
10. Henderson, Amy C. (2003). *Meaningful Access to the Courts.* 72 University of Missouri – Kansas City Law Review 571.
11. Ground Zero for the Secret Service. G4TV, http://www.g4tv.com/techtvvault/features/27904/Ground_Zero_for_the_Secret_Service.html?detectflash=false&.
12. Hine, Kelly D. (1998). *Vigilantism Revisited.* 47 American University Law Review 1221.
13. MSNBC (2006). "Dateline," http://www.msnbc.msn.com/id/10912603/.
14. Perverted Justice, http://www.perverted-justice.com/ (2006).
15. Sidman, Andrew (1975). *The Outmoded Concept of Private Prosecution.* 25 American University Law Review 754.
16. Sklansky, David A. (1999). *The Private Police.* 46 UCLA Law Review 1165.
17. State v. Martineau, 148 N.H. 259, 808 A.2d 51 (New Hampshire Supreme Court 2002).
18. Zentner, Lynn A. & Klumb, Eric (2003). Donated Resources. Washington, D.C.: U.S. Department of Justice.
19. Wikipedia (2006). *Artists Against 419*, http://en.wikipedia.org/wiki/Artists_Against_419.