A Paradigm Shift in Online Policing – Designing Accountable Policing

Nimrod Kozlovski
nimrod@yale.edu

"A Paradigm Shift in Online Policing – Designing Accountable Policing" will appear soon in book form. The table of contents and introduction are attached. If you are interested in obtaining a preprint copy of the entire manuscript, please contact the author at the email address given above.

This work was supported in part by the National Science Foundation's Information-Technology Research program under grant number 0331548.

Table of Contents

Chapter Four – Technology in the Service of Accountability – Watch the Watchers

Introduction

The transition to an information society increases our dependence on communication and computation infrastructures. While the new online environment introduces great opportunities for contemporary society, it also opens up vulnerabilities and changes the types of risks we face. Our information infrastructure was designed with a particular sense of security in mind—assuring the survivability of the network itself—but it has limited built-in guarantees of confidentiality, integrity, and availability. Survivability was the main priority in establishing a military network that needs to function even in time of attacks and failure of nodes. However, the designers of the Internet did not envision it to serve as a platform for civic and global communication and commerce. It was not designed with concerns about users' identification, accountability and trust, which are essential for the kind of network which the Internet has evolved into.

Following the original design principles, the Internet serves as a medium of communication with unique characteristics, different from any medium of communication that preceded it. The internet was designed as a universally open forum which is decentralized, equal among users, interactive, neutral among different applications, (potentially) anonymous, linked, and easy and inexpensive to use. Moreover, it lacks any central control, and resists attempts to gain command over its uses or users. This architecture further promotes interoperability and interconnectivity between different systems and applications, enabling varied equipment and technologies to connect to each other. A medium with such a design carries great promise for empowering the individual, advancing individual creativity, enriching democratic discourse, and fostering innovation. However, a medium of such design also enables malevolent and unaccountable uses of a distinct nature. It has invited a new architecture of crime which poses new and unique challenges to contemporary society.

Cybercrime has become a troubling phenomenon which requires special attention. As I am writing this introduction, newspaper headlines remind us that we can not stay idle in the face of these new patterns of crime. The online theft of 40 million credit cards

information in the U.S. is currently enabling wide scale fraud; introducing questions regarding the future of online payments. At the same time, a large scale network of economic espionage using computer Trojan horses has been exposed in Israel; revealing the dark side of the information environment. Meanwhile, in Britain, critical infrastructure systems have been the target of foreign spying and attempts of malicious attacks. These incidents and many others, including the recently exposed global ring of pedophiles and online organized crime operations, encourage us to think about the unique challenges introduced by cybercrime.

While the perpetrators of cybercrime may aim to accomplish the same malevolent goals as those of offline criminals, they commit their crimes in a very different manner. Online criminals take advantage of digitization, automation, and distributed design to produce crimes of different scale and different damage potential. With the use of encryption and steganography (i.e. unobservability method), online criminals can hide their traces, as well as incriminating evidence that could be used against them. They are also able to use the network design to enjoy anonymity and evade detection. Moreover, online criminals are not bound by physical geography and can inflict harm across jurisdictional borders. By introducing an international element into the crime, criminals are able to enjoy jurisdictional arbitrage of both substantive and procedural law. In doing so, they can complicate the investigation and reduce the chances of successful prosecution. Combined together, all these new characteristics of crime change the potential magnitude of crime, the social organization of criminal activity, and the cost-benefit considerations in committing criminal activity.

The change in the nature of crime demands innovative thinking when it comes to the design of our policing system. It challenges contemporary society to question whether the methods of policing that have served against physical crime are capable of handling cybercrime. It is relatively a short period of time that cybercrime has become a major risk for contemporary society, yet it has already led to revolutionary changes in the ways we police society. Cybercrime has initiated a paradigm shift in policing and is also likely to

have immense impact on the ways in which contemporary and future societies will conceive of real world policing.

Modern societies have been accustomed to a professional law enforcement system. It is a reactive system that responds to a committed crime with a professional policing force. This system is relatively centralized, publicly managed, and rooted in human discretion. It operates by deterring potential criminals with the probability of sanction. If a crime is committed, public police conduct an investigation to trace back to the perpetrator and provide evidence for prosecution. This model of policing has so far proven to be ineffective in controlling cybercrime. With the new conditions of criminal activity, deterrence is not achieved, and investigations are often futile against the sophisticated and determined criminals.

The difficulties of the professional law enforcement system to address cybercrime have led to second thoughts on whether a reactive, public policing system is the optimal system of policing. In practice, we are currently witnessing the end of the professional law enforcement model as we have known it. There are various reasons for that. To begin with, the fundamental assumptions of the professional law enforcement model seem to be invalid online. It assumes deterrence, the possibility of successful investigation and manageable damages of disorder. However, when the criminal can strategically plan the crime to be anonymized, untraceable, encrypted, automated, propagating, distributed and internationalized – all theses assumptions of the reactive system seem questionable. Furthermore, a proactive model of policing becomes economically and technologically more efficient, and potentially less intrusive than traditional law enforcement. It challenges contemporary society to question whether it continues its preference for a second-best reactive system. Last, the institutional arrangements in cybercrime create pressure for a new policing system. The change in the nature of "spaces" and ownership of "spaces" for public interactions logically leads to privatization of policing functions. Private entities have increasingly greater control over the points of efficient policing intervention. They strategically prefer to manage risk with preventive mechanisms than to be assisted with a reactive law enforcement system.

All these forces are currently pushing towards a different system of policing. The emerging system of Cyber-Policing follows a different paradigm than that of the known law enforcement model. The emerging system of policing is mainly proactive, highly decentralized, comparatively more privatized, and to a large extent automated. It is informed by information security strategies. It is much more pervasive than offline governmental law enforcement. It calls for ubiquitous policing of online activities to monitor, control, deter, deflect, detect, prevent, or preempt risky and potentially malicious activities. The new policing system changes from the paradigm of criminal justice to one of security. It favors prevention over detection and punishment.

At the core of the new policing system are proactive tactics of policing. Instead of waiting for a crime to be committed and reacting to it, online policing shifts the initiative from the criminal to the policing force. Policing entities gain access to operational intelligence prior to the commitment of the crime, get control at effective points for policing intervention, and employ crime-oriented policing to respond to the particular patterns of crime. Policing entities, both public and private, simultaneously employ various proactive tactics to address the conditions of particular crimes. Online policing uses statistical predictive models about criminal and anomalous behavior, and build profiles of potential perpetrators. These models and profiles are then run against voluminous databases (mainly of transactional records) to predict crime and sort out potential criminals. Furthermore, online policing heavily employs undercover operations, both human-operated and automated, to entrap potential criminals. In addition, the architecture of the virtual environment (a.k.a. "Code") is designed with the intention of making crime impossible, or to reduce the opportunities for committing crime. Moreover, wired sensors are embedded in the environment to conduct ubiquitous surveillance. The abundance of smart sensors, which are programmed to monitor for a particular activity, enables us to employ this surveillance infrastructure for real-time policing interventions. At the same time, the new policing system focuses on proactive identity control to protect against unaccountable users.

In such a proactive system, the use of sanctions changes its meaning. Sanctions are no longer the traditional legal ones of imprisonment and monetary fines, which are imposed by a judicial body following procedural due process. Online sanctions normally focus on the exclusion of a user, banishment, or denial of permissions. The sanctions are often employed by private parties or the online community, without judicial oversight and function as an immediate constraint for further activity.

The new policing system operates by an institutional design which is very different from the public law enforcement system. Various forms of private organizational structures, for-profit and not-for-profit, operate aside or in partnership with the public police. These operations are often not bounded by jurisdictional lines, and a cross-jurisdictional and supra-national structure, both public and private, emerges. These operations also divert from the common centralized design of the police force, as decentralized structures replace or supplement traditional operational designs.

In this new policing environment, the public police reinvent their role and redefine their relationships with private security. Private security entities are assigned to operate their own risk management and their security operations within their controlled "space". They are further empowered and encouraged to employ coercive policing powers and to sanction users. In this sense, the public police pull out of micro-policing and have entrusted private entities with it. At the same time, the public police acknowledge their important role in macro-policing in an environment with growing interdependencies and the risk of cascading failures. The public police, therefore, manage the overall risk and orchestrate cross-platforms operations.

This new model of policing addresses its challenges relatively efficiently, strategically employing the most effective tools, intervention points, and institutional settings for any given situation. It enables a flexible continuum of policing interventions which replaces the rigid tools of physical enforcement. It creates a policing pattern which is responsive in real-time to changing conditions and to evolving risk patterns.

Furthermore, the new model reduces the costs of policing and more effectively compels the relevant parties to internalize the policing costs of their activities. In addition, it invites relevant stakeholders to be involved in the policing effort and enables them to register their preferences in its design. The new model regains the deterrence lost in the transition to the online environment. With the use of local points of control, such as the ISPs, it also enables to enforce local norms, avoiding the problem of extra-jurisdictional effects. By employing local players and personalizing intervention, it has the potential to target policing to relevant subjects while leaving other users unaffected.

Moreover, this model, if designed with democratic values in mind, can actually enhance privacy by minimizing the collateral effects of policing. It can lead to more precise and more focused interventions that replace the rough tools of current policing. Instead of interfering with innocent traffic to spot criminals, it can filter out only potential criminals, leaving other traffic untouched.

To conclude, the emerging model is better suited to the new information environment than traditional law enforcement, because it understands the nature of the change from atoms to bits, from space to flow, from presence to representation.

However, while the new policing model may seem more effective than the old system of law enforcement, it raises many objections. The new system of policing is emerging with no real guidelines and few restrictions. This system is increasingly in conflict with our values, as well as our normative considerations and expectations from a policing system. It has not been following the established expectations that a policing system will respect the traditional democratic balance between security, liberty, autonomy and freedoms; and further leads to unaccountable policing.

The objections to the new policing system are phrased in connection both to its proactive strategy and to its new institutional structure. As a threshold objection, many have argued about the ineffectiveness or inefficiencies of certain components of the new model. We are reminded to examine each new policing technology; whether it is indeed competent in

achieving its stated goals, and whether the cost of policing does not outweigh the benefits. Aside from these functional objections, there are plenty of objections which relate to the effect of the new policing model on the democratic balance of power. The new policing model extends the infrastructure of social control and tends to remove the limitations that traditionally served to restrain policing powers. The new system expands the sphere of social control through dataveillance, wired surveillance, constraining architecture and the spread of distrust among users. Furthermore, certain tactics of policing, such as predictive data mining, do not follow the form of probable cause and particularized suspicion, and therefore expand the realm of the police also to monitor and potentially chill innocent behavior. In doing so, it changes the conditions of liberty and freedoms in society and expands the coercive powers of the government.

Others have argued that the emerging policing system interferes with established notions of the criminal justice system and with its social role. It substitutes notions of guilt, shame, and mercy with a purely utilitarian system and strips the criminal justice system from its important role in conveying social meaning.

In addition, the new policing system is often objectionable because of its effect on the internet as a medium of communication and platform for innovation. While the new model takes steps to design the environment to accommodate policing interests, it neglects their effect on the architecture of the medium and its political implications. Changing the basic architecture, or interfering with the natural information flow, threatens to deprive society of the benefits of this new medium.

In addition, concerns have been raised against the techno-dependence of the new model. Information technologies are suspicious of having flaws, hidden features or "back doors." They operate in an obscure and impenetrable logic which increases the risk of misuse. Furthermore, once technology is becoming socially accepted as a policing tool, we often tend to be too complacent about it. We tend to over-rely on the technology and stop applying the required judgment in assessing its output. We substitute human discretion with automation, even when the technology has potential failures and imperfections.

Aside these objections to the proactive strategy, there are severe concerns about the shift in institutional structure, the decline of public policing and the rise of private entities that perform policing operations. With the shift toward private policing there is erosion in the protections that guard the individual against coercive policing functions; and the risk to individual liberty increases. Private policing forces tend to lead to discriminatory policing, unequal exposure to policing functions, and disproportional use of coercive powers. Private policing also tends to be less accountable to the public for its actions.

The problem is that while the new model is emerging to achieve better and more effective security, it diverges from established notions of democratic policing. A democratic society is dependent upon effective policing force, as personal liberty and even liberal democracy itself are impossible without competent policing powers. At the same time, democratic society must keep policing powers within defined boundaries to protect individual liberty and freedom. This is the dual notion of policing in democratic society: empowered to keep effective security, but also restrained and controlled. The regulation of policing is aimed as setting a balance between policing functions and liberty and individual freedoms.

A democratic society experiences difficulties when this balance is distorted. It is problematic when the police are either too restricted to perform their tasks, so security can't be achieved, or the policing powers are not properly controlled, so liberty and freedom are endangered. The regulatory forces which enable and restrain policing powers must retain the proper democratic balance. These regulatory forces consist of legal regulation, but also of technological conditions and institutional structures, which enable and restrain policing operations (hereinafter: "regulatory forces"). However, in times of profound change in the social and technological conditions, the regulatory forces may be rendered ineffective and require adjustments or redesign.

With the paradigm shift in policing that is emerging online, the regulatory forces that were designed to enable and restrain law enforcement operations seem inapplicable or

obsolete. The existing regulatory forces are rooted in the operational assumptions of the old law enforcement model. They assume a reactive, public, and centralized policing system. They fail to properly function when these founding assumptions are radically changed. They are incapable of accommodating the change to a proactive, decentralized, and highly privatized policing model.

It is, first of all, the existing legal structure which is ill-equipped to deal with the new policing system. Criminal procedure law is entrusted with the dual task of enabling effective policing operation, but also restraining them so as to protect the individual. It aims to structure a balance to enable policing operations which are reasonable, proportional, and accountable. However, the existing criminal procedure follows the assumptions of the traditional law enforcement model. It is set to protect against a public police force which reacts to committed crime by collecting evidence for prosecution. Furthermore, it has an embedded bias towards physical crime, assuming a physical crime scene and physical evidence. Theses assumptions shape the existing doctrines of criminal procedure.

However, these existing doctrines do a poor job in enabling and restraining the new policing operations. Existing criminal procedure doesn't supply protection against policing functions which are conducted by private parties. It does not protect against the ubiquitous collection of low-level transactional data, which serves in predictive policing. It remains mute when a regulatory effect is achieved through the design of the architecture, and not through enforcement of the criminal law. Further, it doesn't protect against analysis of lawfully acquired information, even when such analysis poses a major risk to individual liberties and freedoms by discovering knowledge that remains obscure in plain data. It provides no protection against the infringement of information privacy which occurs when these bits of information are aggregated together. It supplies no remedy against preventive use of force – such as exclusion and banishment – when it doesn't reach formal prosecution.

In addition to these problems, and many other inadequacies of existing criminal procedures to deal with the new policing environment, recent developments make it even more troubling. Legislators still assume the old policing model, and in order to compensate for the difficulties of law enforcement online have expanded governmental authorities and loosened the constraints on their operations. These changes in the law include: expanding governmental secrecy to inhibit disclosure of policing technologies; expanding records keeping and data retention requirements to insure available information for law enforcement; and, immunity to private parties for policing functions, serving potentially as an over-incentive to engage in those activities. When these developments are added to the aforementioned failure of criminal procedure to protect civil liberties and assure accountability – a troubling picture is revealed.

Aside from the law, technology and institutional structures have traditionally served to restrain policing operations. However, these regulatory forces have also become relatively ineffective in the shift to the digital crime scene. Policing technology has traditionally helped keep policing accountable, when it was transparent and visible and exposed the nature of coercive power. However, with the shift to information-based policing, the technologies in service of policing are less visible and transparent. It is hard to trace or understand intentional, virtual coercive force and therefore to hold it accountable. At the same time, institutional structures have traditionally helped to establish policing accountability in various ways: hierarchy and command structure within organizations; operational walls between departments and functions; and inter-organizational collaborations which exposed policing operations for external review. These institutional conditions have changed in the new policing structure and have also led to an erosion of accountability.

The failure of existing regulatory forces to restrain policing requires us to rethink how to regain control over policing powers in society. In the absence of effective regulatory forces, policing powers operate in conflict with our democratic notions of policing. The regulatory forces no longer supply a solution for the many objections which have been justifiably raised against the new policing system. It is imperative therefore to examine

how to design a regulatory structure that fits the new policing environment and provide an answer for the numerous objections.

So far the attempts to make amendments to the existing regulatory structure have led to unsatisfying results. Policy discussions seem to carry a binary format: either to grant authority to the police to use certain policing tools or to prevent them from using them. When authority is granted, regulations normally create complex authorization procedures. Such procedures tend to impose a bureaucratic burden on the policing force, and stifle the use of effective and important policing tools. They, however, provide very limited genuine protection for individual freedoms. Furthermore, these regulations tend to focus on legal rules and fail to acknowledge the importance of technology and institutional structures in controlling policing operations.

In this project, I challenge this regulatory mindset. I argue that instead of focusing on ex-ante authorization of policing activities, we should better focus on proper accountability for these operations. I further argue that we need to think of law, technology and institutional structures as working in tandem to establish the proper regulatory structure. To make it clearer: I do suggest that certain technologies should not be legal for policing operations regardless of their effectiveness, because of their implications on liberty and freedoms. However, when, after an open public debate, society decides to approve of the use of a certain technology, the preference should be for ongoing accountability of the usage, rather than a one time, ex-ante, authorization procedure. Accountability mechanisms should be incorporated in the technology itself, in the institutional design, and in the legal regime that regulates them.

Accountability, as I define it, is first of all answerability. It is the responsibility to account for actions taken as well as inactions, so as to enable oversight. It is the responsibility to provide evidence which may be accompanied by a requirement to explain or justify actions. It is also to expose one's actions and inactions to review and possibly to sanctions. Accountability mechanisms are the rules, processes, technologies, design principles or institutional structures that hold an entity to account for its actions and

inactions. It can be, for example, a reporting requirement, a technological feature that logs the use of a policing tool, or a civilian oversight body.

I believe that mechanisms that are set to establish accountability have the potential to balance policing efficiency and civil liberties. These accountability mechanisms hold the promise to provide an appropriate response to the many objections raised against the new policing system. Accountability mechanisms expose policing technologies and operations for public review. They facilitate a public debate about the effectiveness and efficiency of these technologies, as well as their effect on the democratic balance of power. They publicly expose the nature of coercive power and enable the ongoing questioning of its desirability. These mechanisms can monitor and alert about possible misuse or abuse of policing powers. They deter those who are invested with policing powers from overstepping their authority. Furthermore, they are capable of addressing the concerns about the techno-dependence of the new policing model, assuring reliable policing tools and routine human control over technological processes.

Well-structured accountability rules can serve to substitute existing authorization rules which seem ill-suited to the needs of online policing. In other words: it is my belief that properly functioning accountability measures can compensate for the relative weakness of authorization rules. A policing authority that faces fewer restrictions on its power must be subject to tighter control of its operations. Accountability rules, that work to routinely and continuously monitor policing, can enable effective policing operations, while at the same time holding them to close review. They can operate in the background without interfering with policing functions, but insure that they are carried out according to the democratically defined limits. In this sense, accountability mechanisms truly live up to the dual mission of democratic policing. Furthermore, accountability mechanisms can support newly developed privacy enhancing technologies. Technologies of this kind, such as anonymization of data or analysis restrictions, embed the protection of privacy within the policing tools themselves. Accountability mechanisms assure us that these technologies are properly used, and that privacy enhancing features are appropriately implemented, configured, and employed in the policing operations.

Accountability mechanisms are by no mean a new concept in democratic policing. Accountability is a concept rooted in offline policing operations, and ingrained in their regulation. The police have always followed auditing, control, and oversight procedures, both internal and external, which have assured accountability. Yet, these mechanisms have attracted only limited scholarly attention, and are often perceived as technical and bureaucratic procedures. It is time to reconsider their role in controlling policing operations in the new environment. Properly designed accountability mechanisms can take advantage of the potential of information technologies to provide automated, tamper-proof, timely and comprehensive logs for policing operations. They can support internal control mechanisms and facilitate external audit and oversight.

However, while accountability mechanisms should be assigned a prominent role in restraining policing, they haven't properly transferred from the offline policing environment. At the moment, we certainly do not take advantage of the potential for increased policing accountability that information technologies can provide society with. Established auditing and control processes haven't been sufficiently incorporated in the new policing environment. Furthermore, the shift to new policing tools has enabled law enforcement to unchain itself from rigid procedures that have assured accountability of traditional policing operations. Policing technologies have been developed with no attention to accountability and this has led to accountability deficit in the new environment. The legislators and the courts have further contributed to this accountability deficit. Instead of demanding accountability mechanisms for the new policing environment, they have structured additional layers of authorization or indirect reporting requirements which provide a poor substitute for accountability mechanisms embedded within the technology.

It is time to rethink accountability. We need to think creatively how to design accountability mechanisms that fit the new environment and live up to the potential of new information technologies. We need to think how legal, technological, and institutional designs can work in tandem to create a strong environment of policing

accountability. In this process, I recommend to focus on the potential of the technology to be in the service of accountability. A well thought technological design can help us watch the watchers.

I recommend that accountability values inform the design and implementation of information systems for policing. We need to consider technological accountability in two aspects: the design of the tools and their actual usage. Accountability for the tools focuses on general disclosure of the functions and capabilities of the technologies which are used for policing. Accountability for the technology may include disclosure of its source code, design principles, configuration, performance measures, and the user's manual. The second dimension of accountability focuses on the particular instances of use (or misuse) of a technological tool. Accountability in this sense is facilitated by a technology that logs and audits the use of each device in particular policing operations.

I argue that policing information technologies and surveillance tools which operate as black-boxes are in conflict with basic principles of democratic policing. In order to gain legitimacy and to serve accountability, policing technologies must be more open and transparent. Disclosure of the source code of the tools and their technical details should be the rule, and controlled disclosure should be the exception. Even when security concerns call to protect the disclosure of the source code, an alternative to full disclosure must be structured to insure accountability.

In addition, I argue for the design of comprehensive accountability mechanisms in the policing technologies themselves. I detail the design guidelines for such technologies. We should have audit trails that are comprehensive, adjusted to the risks of the systems, and tamper-proof. We should have logs that support internal supervision and control and external oversight. We should establish internal procedures to analyze and systemically check the logs to detect anomalies and potential misuse. We should establish external auditing bodies to conduct random checks and supervise the internal auditing procedure. We should prevent destruction of logs or manipulation of reports and deter such acts. We

should also require regular reports that account for the audited activity, as well as detailed reporting without disclosing sensitive and protected information.

In my vision, technology should be assigned the primary role in providing accountability. However, I also advocate for legal mechanisms to support design for accountability, and to promote a culture of accountability. The law should state the accountability measures that must be incorporated in the technology and specify logging, auditing, control, and reporting functions. The principles of reliable auditing must be incorporated into the law rather than being left to the police's discretion. Moreover, the law should include clear standards for the retention and preservation of accounts, and impose sanctions for the failure to keep audits and for the destruction of these accounts. I further recommend redesigning existing legal procedures and litigation processes to promote accountability. I conclude by drawing the guidelines for new evidence law, discovery rules, search and seizure procedures, freedom of information rules, and identity attribution processes; all of which can better serve accountability.

A Road Map

The argument of this dissertation unfolds in four chapters: Chapter One introduces the digital crime scene and encourages us to rethink crime in the digital environment. It lays out the design principles of the Internet and analyzes how this architecture interplays with the nature of online crime. It then continues in detailing the unique characteristics of cybercrime and explores their implications for existing law enforcement operations.

Chapter Two explores the paradigm shift in policing that is emerging as a reaction to the new crime scene. It describes and analyzes the shift from the Professional Law Enforcement Model of policing to Cyber-Policing. Drawing on a historical perspective, it deconstructs the professional law enforcement model to its basic building blocks. Later, it analyzes why a model of policing with such characteristics is unlikely to be the prominent model of online policing. Then, it turns to describe the emergence of a new model of policing which is gradually replacing the old law enforcement system. It

carefully studies the elements of this emerging model, both in terms of strategy and institutional structure.

Chapter Three discusses the objections to the emerging system of policing and examines why existing regulatory forces do not supply an adequate response to these objections. Part one of this chapter develops a functional taxonomy to study the various objections to the new model's proactive strategy and hybrid institutional structure. It starts from threshold functional objections such as effectiveness or efficiency. Then it progresses to introduce normative objections, including the distortion of democratic balance of power and notions of criminal justice; political economy implications of tampering with Internet's architecture; and the alarming techno-dependence of policing. This part concludes by examining the objection to private policing structures on grounds of equality, accountability, proportionality and fairness.

Part two of the chapter aims to understand why existing regulatory forces, which are designed to enable and restrain policing powers, are rendered ineffective in addressing the aforementioned objections. It studies the failure of current legal regulations to capture the potentially troubling attributes of the new policing system. It continues by examining the role of technological transparency in controlling policing operations. It then analyzes how the lack of transparency and visibility in information technologies in the service of policing leads to erosion of accountability. Lastly, it examines why newly emerging institutional designs are incapable of restraining policing powers.

Chapter Four explores potential paths in restructuring regulatory forces with the aim of achieving democratic policing; policing powers which are effective in achieving security and at the same time are restrained and held accountable. It argues for a necessary change in the regulatory mindset, from one of authorization rules to one of policing accountability. It studies the importance and the potential of properly functioning accountability mechanisms in sustaining democratic policing. However, this chapter identifies a failure in the transfer of accountability mechanisms from the physical to the online policing environment. It, therefore, encourages us to rethink accountability in the

online environment and draws the design principles for the restructuring of accountability mechanisms. It explores the prominent role of technological design in watching the watchers, and draws specific recommendations for accountability mechanisms to be embedded within policing technologies. The chapter concludes by discussing the legal rules that should support this technological design in establishing an environment of policing accountability.