

## **Designing Accountable Online Policing/ Nimrod Kozlovski<sup>1</sup>**

### Abstract

We are in the midst of a paradigm shift in law enforcement. The online crime scene introduces complex challenges to law enforcement that inevitably lead to the emergence of a new policing model. The strengths of the emerging model derive from employing alternative strategies of law enforcement. Yet, many of the model's features escape the restraints which limit the use of policing power. It is possible to have a more secure environment, which simultaneously enhances liberty, but in order to achieve that, it is imperative to design an accountable policing model.

In a democratic society, those invested with policing power must be held accountable. At the heart of accountability is the notion of answerability. Accountability manifests itself in responsibility to account for actions taken and actions not taken, and to explain or justify them. It is the duty to expose oneself to review and the possibility of sanctions. Accountability mechanisms are essential to protect civil liberties from infringement, deter policing from abuse of power, promote efficiency, and open a democratic dialogue.

Accountability is a relational concept. The accountability of the individual, law enforcer and omnipresent online third parties all interact with each other. The overall levels of reciprocal accountability of all parties form a dynamic equilibrium, which balances liberty and security in society. Currently there is a race to the bottom, as the new environment enables all parties to erode accountability. My proposed solution ties users' traceability with policing accountability and offers a viable equilibrium in which liberal democratic values can be secured.

---

<sup>1</sup> Nimrod Kozlovski is a fellow at the Information Society Project, Yale Law School, and an adjunct professor of law, Cybercrime and CyberTerror at New York Law School. This paper is part of a research towards J.S.D. dissertation at Yale Law School.

I am grateful to Professor Jack Balkin, the Director of the Information Society Project, Professor Yochai Benkler, and Eddan Katz, Shlomit Wagman, Tal Zarsky, Gal Levita and Caio Mario da Silva Pereira Neto, fellows at the Information Society Project, for their invaluable comments and suggestions.

Now, when the technology for the new policing model is still being developed, is the time to design the measures that will ensure accountable policing. The design stage must be informed by accountability values. The development of new technology invites the establishment of new institutions to supervise policing, and value-driven design may enable new legal procedures that are better equipped to hold policing accountable. It is in our hands to design the desirable policing system.

### Structure

The first part of this paper describes the paradigm shift in online policing. It starts by introducing the need within the new CyberCrime scene for rethinking policing. It continues with a description of the policing model which is emerging online and portrays its distinctive features: prevention through patterns; alternative restraints to crime; private-public policing; decentralized vs. centralized design; regulating victims and third parties; information sharing; self-help sanctions; regulating identification; and non-content analysis. It then analyzes how the emerging policing model withstands performance challenges.

The second part discusses the problem of unaccountable online policing. It explores the potential problems with the emerging policing model, and its tendency towards unaccountable policing, and investigates the current failure in holding policing accountable in three layers: legal, technological and institutional.

The third part examines the concept of online accountability. First, the essence of accountability and its benefits are examined. This further reveals the nexus between accountability and transparency and analyzes how accountability systems work. Then it discusses accountability in the online environment as a dynamic equilibrium between users, law enforcement and third parties. It looks at the normative continuum of accountability and explores the problem of accountability arbitrage in this context. Finally, it turns to the lack of users' accountability which distorts the equilibrium and offers a solution of a users' traceability model tied to policing accountability.

The fourth part focuses on specific design proposals for accountable online policing. The proposed design guidelines for accountable policing include: Optimal equilibrium; Liberal accountability values; Medium sensitivity, Circumvention analysis; Functional equivalency; Layers of accountability, and Continuum of accountability. In this part, design stages are analyzed with a view towards improved accountability for the new policing model in three parts: (1) Technology which facilitates the design of new supervising institutions; (2) Technology which facilitates new legal accountability regime with a focus on search and seizure law and the structure of judicial review; and (3) Regulatory methods to hold private policing accountable such as: agency rules; liability and openness; consented searches; and fair information practices.

## **I. Paradigm Shift in Online Policing**

### **A) New crime scene requires rethinking policing**

The rise of a new policing system can be primarily attributed to the features of the online environment – digitization, anonymity, connectivity, mobility, decentralization and interdependence - which change the crime scene and the map of threats.<sup>2</sup> The new crime scene requires law enforcement to reassess vulnerability and risk<sup>3</sup> and to reconsider effective points of intervention.<sup>4</sup> The technological structure of the network makes omnipresent third parties, such as Internet Service Providers (ISPs) and DNS routers, essential to the operation of policing. It further introduces powerful nodes into the network as information gatekeepers, such as portals, search engines and dominant websites, which can be utilized for law enforcement. The technology is constantly progressing to crime prevention,<sup>5</sup> but works within the existing legal constraints, and demonstrates weakness in tracing criminals and facilitating prosecution.

Aside from the changes in the crime scene, the lessons of offline enforcement and the advancement in the understanding of criminal behavior have led to innovative thinking in terms of designing the policing regime for the new environment. Disillusion with the traditional deterrence model, disengagement from notions of criminal justice like rehabilitation and the appearance of community policing theories inform the design of online policing. The new environment in its formative stage can be understood as experimental ground in which constant simulations of alternative policing methods are examined and studied.

---

<sup>2</sup> See: Neal Kumar Katyal, “Criminal Law in Cyberspace”, 149 U. Penn. L. Rev. 1003 (2001).

<sup>3</sup> Abusing common vulnerabilities, wrongdoers can pose asymmetric risks to other users and create damages with cascade effects, while potentially remaining untraceable and out of the reach of law enforcement. See: Scott Charney, “The Internet, Law Enforcement and Security”, 662 PLI/Pat 937 (2001).

<sup>4</sup> The challenge is to find effective centralized intervention points in a decentralized environment. Current research on the actual ecology of the information environment enables us to identify power laws and patterns of centralization on the Internet. See: Bernardo A. Huberman, *The Laws of the Web – Patterns in the Ecology of Information* (MIT Press, 2001).

<sup>5</sup> See: K.A. Taipale, “Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data”, 5 Colum. Sci. & Tech. L. Rev. (2003). For technical background, see: Jesu's Mena, *Investigative Data Mining and Crime Detection* (Elsevier Science, 2003).

Gradually, developments in the methods of addressing online crime, form a fundamentally distinct system of law enforcement. The fundamental notions in the operation of law enforcement are being gradually abandoned: its basis as a public operation run primarily by the government; that private parties' use of force shall be limited and contained; that bringing criminals to justice is the goal; that human discretion is essential to the just operation of law enforcement; that positive requirements of reporting crime or preventing crime are the exceptions; and that criminal law adjudicates ex-post a criminal act but does not act as a prior restraint.

### **B) An Emerging Policing Model**

Methods of law enforcement that are developing to tackle the exponentially growing phenomena of cybercrime introduce a unique challenge for the legal scholar. She may notice a deviation from common enforcement practices that she observed offline, but looking at a single instance through the lens of offline enforcement models, she will not be able to understand the way in which this deviation fits in to the full puzzle of a new system. To fully understand virtual law enforcement, we need to relax our assumptions of traditional law enforcement and seek to draw together seemingly unrelated pieces of information to form a complete picture. Only then we will be able to notice that the features of online law enforcement operation emerge to form a system of policing that is substantially different from traditional offline enforcement.

This section aims to describe the emerging policing model and to introduce several distinct features of online policing operation.<sup>6</sup>

***Prevention through patterns*** - Policing aims towards prevention and preemption of crime rather than towards prosecution. To predict crime, automated tools constantly monitor the environment to rank user's risk profile against dynamically-identified

---

<sup>6</sup> The identified changes in law enforcement operation initiated from policing efforts to combat cybercrime. However, their rationale expands to combating information-intensive crimes and further informs the general discussion on law enforcement online and offline alike. Information-intensive crimes are defined as crimes that normally leave a distinct information trail and their investigation requires the analysis of vast amount of information to identify the crime pattern. Money laundering, credit card fraud, and anti-trust violations tend to be information-intensive crimes.

patterns of criminal behavior. Further, they monitor for anomalies or deviations from “normal” behavior. Proactive tools act upon identified risk to preempt potential crime.

***Alternative Restrains to Crime*** - Policing heavily employs and supports non-legal restrains to crime. Law enforcement recognizes in virtual space a toolkit of restrains to criminal behavior which vary from law to the features of the technology, the design of the network’s topology and the social construction of the use. Therefore, law enforcement strategically shifts to design the technological and social construction of the environment to tackle crime.<sup>7</sup>

***Private-Public Policing*** - Policing operates institutionally in a hybrid of public and private enforcement. From relatively centralized public efforts to combat crime, with limitations on the delegation of policing power to non-public entities and fairly strict restrains on the private use of force, the growing tendency is to shift policing responsibilities and rely on the private sector’s efforts,<sup>8</sup> The shift towards the private sector is conducted in four distinct methods: partnership, delegation, imposition of responsibilities, and privatization of enforcement. New policies are specifically tailored to increase private enforcement efforts to enjoy their relative advantage in assessing vulnerabilities, collecting intelligence, conducting surveillance, analyzing data, restraining deviant behavior, and operating undercover entrapments.

***Decentralized vs. Centralized Design*** - Policing is shifting to a hybrid architectural structure that enjoys the relative benefits of decentralized and centralized topologies of policing networks for different tasks. The main policing effort operates in a structure which optimizes the allocation of responsibilities between the hubs and the edges. The topology of operation allows law enforcement to enjoy the relative advantage of the edges in sensing their local environment, analyzing risk in context, and using force in

---

<sup>7</sup> See: Joel R. Reidenberg, “States and Internet Enforcement”, 1 Univ. Ottawa L. & Tech. J. (2004); Neal Kumar Katyal, “Digital Architecture as Crime Control”, 112 Yale L. J. 2261 (2003). For a general discussion on the nature of regulatory forces online, see: Lawrence Lessig, Code – and Other Laws of Cyberspace (1999), Chapter 7.

<sup>8</sup> Michael Birnhack & Niva Elkin-Koren, “The Invisible Handshake: The Reemergence of the State in the Digital Environment”, 8 Va. J.L. & Tech 6 (2003).

real-time to mitigate damage. At the same time this structure also empowers the center, by establishing real-time communication with the nodes which enables centralized defense mechanisms, such as segregation of infected area, blockage of certain domains, or centralized distribution of updated defense tools to the edges.<sup>9</sup>

In addition, a fully distributed private architecture is emerging to facilitate correlated vulnerability assessment and joint defense strategies. This architecture creates a peer culture of security.<sup>10</sup>

***Regulating Victims and Third Parties*** - Law enforcement shifts from mainly regulating the criminal behavior to regulating the behavior of the victims and third parties of the crime scene.<sup>11</sup> These regulations aim to create optimal behavior on the part of the victim and to employ third parties for crime prevention and detection, as well as damage mitigation and prosecution-support. Third parties are clustered into groups based on their role: conduits, service providers, information gatekeepers, traffic routers, tool suppliers, and payment systems. They are regulated in three axes: liability, operational requirements and incentives structures.<sup>12</sup> Liability imposed on third parties can take the form of direct liability (e.g. for clearing illegal transactions)<sup>13</sup> or conditioned secondary liability (e.g. notice and take down requirement). The operational requirements vary from requirements

---

<sup>9</sup> It is illuminating in this context to learn from the Pandemonium design concept, *see*: Branden Hookey, *Pandemonium: The Rise of Predatory Locales in the Postwar World* (Princeton Architectural Press & Rice University School of Architecture, 1999).

<sup>10</sup> A recent decision by the Israeli Magistrate Court emphasizes the importance of a peer security culture in an interdependent environment. The court denied the prosecutor's claim that mere port scanning should be defined as an illegal attempt to commit unauthorized access to computers. The court found port scanning to be an essential tool for peer to check each other's systems' security and concludes that appropriate public policy should encourage it as users are best positioned to identify vulnerabilities and security flaws [C.C. 03047/03 State of Israel vs. Abraham Mizrahi (Jerusalem Magistrate Court, 02/29/2004, TBP) (Hebrew)].

<sup>11</sup> *See*: Joel R. Reidenberg, *Supra* note 7; K.A. Taipale, "Internet and Computer Crime: System Architecture as Crime Control" (Feb, 2003) (Available at: <http://www.taipale.com/papers/CrimeControl.pdf>); Neal Kumar Katyal, *Criminal Law in Cyberspace*, *Supra* note 2.

<sup>12</sup> Additionally, volunteerism by third parties to assist in enforcement is very common at a time of an increased national security threat.

<sup>13</sup> *See*, for example, the Assurance of Discontinuance, in lieu of commencing statutory proceedings which was accepted by the attorney general of New York State in the case of PayPal, Inc. The agreement with PayPal relates to clearing gambling transactions. (<http://www.dag.state.ny.us/Internet/litigation/paypal.pdf>) (see in particular articles 20-21 to the agreement).

to design or adjust systems in order to facilitate enforcement,<sup>14</sup> to retain logs and traffic data,<sup>15</sup> to dynamically block illegal communication,<sup>16</sup> or to reroute traffic from designated domains.<sup>17</sup> Incentive structures can function in various ways from subsidizing operational costs related to enforcement, awarding immunity from civil liability for enforcement-related activities, and prioritizing law enforcement treatment to cooperating entities.

A common pattern in the regulation of third parties is to grant immunity for third parties vis-à-vis the users while simultaneously imposing new obligations vis-à-vis the government, obligations which rely on the given immunity. Moreover, the regulation often assures the secrecy of the interaction with law enforcement to secure the third party's interest in non-disclosure.

***Information Sharing*** - Law enforcement shares information and dissolves reporting bottlenecks vertically and horizontally. Law enforcement opens bi-directional information channels to share policing-related information with the private sector. It also sets the platform for peer reporting in the private sector. New reporting obligations are imposed to enable real time sharing of information about vulnerabilities, risk and defense mechanisms. In addition, law enforcement information opens to upstream and downstream analysis, both publicly and privately.<sup>18</sup>

***Self-Help Sanctions*** - The essence of the use of force changes online. Traditionally, sanctions in the offline world are imposed publicly by a judicial body through legal

---

<sup>14</sup> The general act which regulates it is the Communication Assistance for Law Enforcement Act (CALEA) (HR 4922). See: Center for Democracy & Technology, CALEA Background ([http://www.cdt.org/digi\\_tele/background.shtml](http://www.cdt.org/digi_tele/background.shtml)).

<sup>15</sup> See: Clive Walker & Yaman Adkeniz, "Anti-Terrorism Laws and Data Retention: War is Over?", Northern Ireland Legal Quarterly 54 (2), Summer Edition, 159 (2003).

<sup>16</sup> See: 18 Pennsylvania Statutes § 7330 (2002). The Center for Democracy & Technology currently questions the validity of the statute in court. See: CDT & ACLU Memorandum in the case: Center for Democracy & Technology vs. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania (E.D. Pennsylvania, No 03-5051).

<sup>17</sup> A central point, such as DNS server or ISPs, can reroute traffic from designated domains.

<sup>18</sup> The tools for information sharing are adjusted to enable flexible sharing policies. By using tools of data anonymization, layer-specific and rules-based access authorization, the information can be opened to variable levels of access to fit the position of the user, its needs and privacy and trade secret interests. See the comprehensive report by the Markle Foundation Task Force on National Security in the Information Age: "Creating a Trusted Network for Homeland Security" (December 2<sup>nd</sup>, 2003) (available at: <http://markletaskforce.org>).

process and tend to carry the form of imprisonment or monetary fine. Online, sanctions tend to carry the form of upfront exclusion, blocking or “virtual imprisonment”<sup>19</sup> and are often imposed by private parties without judicial overview, and sometimes even without awareness of the sanctions taking place.

***Regulating Identification*** - The law enforcement effort focuses on correlating an online identity to a real-life person. In order to facilitate this, it regulates the construction of online identity and identity management.<sup>20</sup> The flexibility of identity construction online and the ease of impersonation create a challenge to security which requires consistent identification, trusted identities and traceable users. Often, the attribution of online activity to a real-life person is the missing dot in investigation. Therefore, new legislation aims to regulate the construction of identity and to further assure traceability. The law is gradually being set to require a traced-back route, to prevent spoofing and misleading identification, and to limit the construction of multiplied identities.<sup>21</sup> Furthermore, the law creates incentives to adopt more secure identification technologies.<sup>22</sup>

***Non-Content Analysis*** - Law enforcement redefines the data building blocks for crime analysis and data sources. As digital data is layered and automatic meta-data is attached to communication, the tools of crime analysis change. The investigators focus on “non-content” data, as traffic data and automated system logs to create maps of associations, and to visualize sequencing and causality charts. This data is further used for risk profiling and risk rating and to locate the optimal intervention point. This data is

---

<sup>19</sup> See: Richard Jones, “Digital Rule – Punishment, Control and Technology”, *Punishment and Society*, Vol. 2 (1) 5-22.

<sup>20</sup> The focus on the identification process is based on the understanding of its potential vulnerabilities. Successful false identification on the part of the criminal enables him to commit a chain of proceeding crimes. Our contemporary society over-relies on identification processes, even when conducted with poor identification means which were not originally created for identification (e.g. social security number). This introduces a major security flaw, which current law enforcement initiatives try to tackle. The initiatives try to identify patterns of identification which are suspicious and to cross-check identifying information with external sources.

<sup>21</sup> See: Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003 (SPAM-CAN Act, 2003), Sec 4 § 1037, Sec 5.

<sup>22</sup> The law creates incentives to use secured identification systems, such as digital signatures, by requiring them as the mean to conduct transactions with the government or by giving them a preferred evidentiary status. Comparative analysis of Digital Signatures laws reveals that legislators worldwide were reluctant to require the general use of digital certificate, and adopted instead the incentive structures to foster the use of the technology.

regularly in the possession of third parties along the communication route and therefore retrieved not from the crime suspects and normally without their notice.

These features assemble together to form a new policing model which has noticeable advantages and disadvantages.

### **C) The Emerging Policing Model Withstands the Performance Challenges**

The emerging policing model turns out to address the new challenges relatively efficiently. It shifts towards dynamic policing which strategically employs the most effective tools, intervention points and entities for any given situation. It creates a policing pattern which is responsive in real-time to the changing conditions of the environment and to the evolving patterns of risk. It is capable of correlating analysis of identification patterns, behavioral patterns, association patterns and application patterns to produce a unified comprehensive risk analysis. Furthermore, it reduces the costs of policing and more effectively compels the relevant players to internalize the policing costs of their activities and deters the infliction of negative externalities on innocent users. Moreover, it invites the relevant stakeholders to be involved in their policing effort and enables them to register their preferences in its design. The new model regains the deterrence which is diminished online and makes it scalable and applicable to other crimes while exploring the nexus between the online and offline environments.

This model also enables the creation of local policing with localized norms, which evades the problem of out-of-jurisdiction effects. By employing the local players and personalizing the intervention, the model has the potential to target policing to the relevant subjects and leave unaffected the rest of the users.<sup>23</sup>

---

<sup>23</sup> The regulation of gambling could serve as a good example. When law enforcement effort targets a gambling website, it creates a problem of over-blocking the site also to subjects of jurisdictions which allow gambling. By shifting to regulation of local third parties much of the gambling in the jurisdiction can be solved. The regulator forbids the credit card companies or other payment systems from clearing gambling transactions for people within the jurisdiction. It further requires service providers to block access of users to pre-identified domains of gambling sites and can require proxy DNS servers to reroute traffic from these domains. The regulation can further target local portals and local search engines which will be forbidden from linking to these sites. Even if savvy users can circumvent this regulation, for most subjects the regulation is very effective.

Moreover, the 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 focused policing interventions to replace the rough tools in service of current policing.

---

However, these modes of regulation may be objectionable for other reasons and may serve tyrannies in disciplining their subjects. For that reasons we may object these modes of regulation, even if they are efficient. This point deserves a separate discussion.

## II. Unaccountable Online Policing

### **A) The Emerging Policing Model – Towards Unaccountable Policing**

This emerging policing model invites numerous objections and may very well lead to severe infringements upon civil liberties. *First*, it provokes excessive use of power by private entities which can create inequality in enforcement, disproportional and untamed use of force, and biased policing. *Second*, with the use of sophisticated sorting tools, it introduces the potential of constant profiling and systematic exclusion of segments in society. *Third*, it might limit liberty and discipline behavior by the “tyranny of the pattern”, such as monitoring on the part of enforcement a deviation from pre-identified patterns of “normal” behavior.<sup>24</sup> *Fourth*, it exposes the individual to extensive surveillance and control since constant monitoring is required to facilitate the model. *Fifth*, it opens the door for hidden surveillance and invisible use of force which is associated with illegitimate regimes. *Sixth*, it enables the government to employ code to extend its reach and to regulate beyond the boundaries of the law.<sup>25</sup>

This model also enables the government to circumvent existing limitations on policing power by employing “Regulatory Arbitrage”: The same policing effect is achieved without having to withstand the restraints imposed on the state. The government can, for example, systematically use personally identifying information collected by commercial entities while avoiding the constitutional and legal limitations that would regulate direct governmental surveillance.<sup>26</sup> This expands policing power and distorts the balance between policing and liberty in society.

---

<sup>24</sup> Policing by monitoring deviation from “normal” patterns might also lead to stagnation and might stifle creativity in society. Creativity is identified as an innovative manner in which to conduct an activity or express an idea. The inherent feature of creativity is employing out-of-the-box thinking and deviation from common patterns. Furthermore, policing by patterns fixates and perpetuates existing power structures as it reflects the notions of those who have power. It imposes an obstacle to those who challenge these notions.

<sup>25</sup> See: James Boyle, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hard Wired Censors”, 66 U. Cin. L. Rev. 177 (1997).

<sup>26</sup> See: Ernest Miller and Nimrod Kozlovski, “eBay to Law Enforcement – We’re Here to Help”, Lawmeme, Feb 17, 2003 (available at: [http://research.yale.edu/lawmeme/mo\\_dules.php?name=News&file=article&sid=925](http://research.yale.edu/lawmeme/mo_dules.php?name=News&file=article&sid=925)); and the following discussion: Slashdot, “Ebay’s Flexible Privacy Policy” (available at:

A closer look at these objections to the emerging policing model reveals that they commonly focus on its potential towards excessive policing and the expansion of power beyond the democratically decided limitations on liberty. The fear expressed is that of over-policing channeled through hidden or unregulated modes of operation. This is the fear of embedded restraints on action which are invisible and hard-wired into the environment.

It is both the dehumanization of power encoded within technology and the privatization of power which intensifies the outcry. It is the resentment of a policing power which is not held to account for its actions and not required to justify its decisions. This is the objection to unaccountable policing.<sup>27</sup>

Accountability is best defined in terms of answerability. It is the responsibility to account for actions taken or not taken, so as to enable oversight. It is the responsibility to provide accompanying evidence with the requirement to explain or justify actions or inactions. It is the exposure of one's actions and inactions to review and possibly to sanctions.

Unaccountable policing contradicts the core principle of democratic society that with power comes responsibility. Power in democracy is interwoven with restraints. The emerging policing model evades accountability. While it shifts from the foundations of the traditional policing model to tackle the challenges of the new crime scene, it also escapes the net of accountability originally designed to keep policing in check.

## **B) The Failure to Hold Policing Accountable**

Existing accountability measures fail to address the paradigm shift in law enforcement for various legal, technological and institutional reasons.

---

<http://yro.slashdot.org/yro/03/02/20/1347252.shtml?tid=158>); Yuval Dror, "Big Brother is Watching you and Documenting", Haaretz (available at: <http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=264863&contrassID=2&subContrassID=5&sbSubContrassID=0&listSrc=Y&itemNo=264863>); Ernest Miller, "Defending eBay?", Lawmeme, February 20<sup>th</sup>, 2003 (available at: <http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=941>)

<sup>27</sup> For discussion on the necessary focus on accountability, see: Amitai Etzioni, "Implications of Select New Technologies for Individual Rights and Public Safety", 15 Harvard J.L. & Tech 257 (2002).

***(1) Why Does the Law Fail to Hold Policing Accountable?***

Legally, the accountability structure is based on the assumptions of offline law enforcement models: it assumes a prosecution-based system, an enforcement conducted mainly by public law enforcement, judicial overview encoded into the procedure, and notification of the subject of enforcement as the interested party in objecting to the enforcement. These assumptions are all placed in question under the new policing model.

*Prosecution law and preventive policing* - Along with a shift from the prosecution-based model to a preventive model legal accountability is eroded. The current legal structure presumes that by assigning evidentiary implications to the failure to follow the legal requirements, the law enforcer ex-ante has the incentive to follow the procedure. Evidentiary rules, such as the fruit of the poisoned tree, which excludes evidence obtained illegally, acts as a deterrent to illegal enforcement methods. The model which has reasonable logic in deferring the sanction on illegal enforcement to the trial stage has no bite when the enforcement effort is not aimed at prosecution.

*Unregulated Private Policing* - The regulation of policing has not kept pace with the institutional tendency to shift towards private enforcement. The legal accountability structure is set on the assumption that law enforcement is conducted primarily by public officers while constitutional guarantees as well as extended legislative protection secure an individual's rights.<sup>28</sup> Specific agency rules apply to the use of private entities for law enforcement assignments to assure the same legal protections are extended and to prevent the government from intentional use of private parties to bypass constitutional and legal constraints. This legal structure becomes questionable as private policing prevails and when mere application of agency rules fails to catch the complexity of the policing endeavor in the accountability net.

---

<sup>28</sup> For a comprehensive discussion on privatization and structure of accountability, see: Jerry L. Mashaw, "Contracting Out and the Structure of Accountability" (Draft dated 09/09/03, presented at the Yale Faculty Workshop).

*Rigid Binary Doctrines* - The binary structure of legal doctrines enables various investigative techniques to fall outside of the accountability net. The legal structure is built on dichotomies: search/ non search; private space/ public space; content/ non-content; expectation of privacy/ no expectation for privacy. These dichotomies lead to binary doctrines which are too rigid to handle the complexity of the new technological environment and too often deem a policing practice to be fully unregulated.

*Outdated ladder of Accountability* - Technological changes have lowered the level of accountability which law enforcer needs to withstand under regulated practices. The lowered standards also often imply that the judicial review is replaced by more lenient administrative mechanisms of review. The criminal procedure is structured according to a ladder of accountability which imposes different bars of accountability on different investigation activities. The accountability standard is based on various factors which are taken into account in the authorizing act: the type of information (user information, non-content information or content); the potential infringement on civil liberties, the intrusiveness of the act, the entity which possesses the information, the severity of the crime, the scope of existing evidence, and the stage of the investigation. The ladder of accountability informs the required procedure that the law enforcer has to follow and the level of justification required to authorize the act. Different procedures lead to the issuance of different legal orders (e.g. search warrant vs. subpoena). The erosion in accountability occurs when changes in technology, institutional setting or business practices enable the bar to be lowered for any given activity.<sup>29</sup>

*Alternative Policing Restraints* - The law fails to hold accountable governmental actions that aim towards policing but which are carried out through non-traditional policing operation. As the government moves towards using disciplinary measures such as

---

<sup>29</sup> Thus, for example, the shift towards remote storage and e-services enables the government to acquire the information from third parties with a subpoena (or sometimes even without it) rather than obtaining a warrant to search the user's computer. Similarly the storage of logs of accessed web pages on the service provider server enables the government to acquire the stored information from the service provider rather than obtaining a wiretap warrant to intercept user's communication.

technological features and architectural design, the current law is ill-equipped to conceive of those measures as policing actions which require careful legal attention.

*Artificial Consent* - Liberal foundations of the law which protect autonomy and set the boundaries between the individual and society are turned on their head in the new environment and are used to subject the individual to power. Consent is a core legal concept which protects individual autonomy from external power. However, legal doctrines, as they developed, deprive the individual from a meaningful choice whether to consent or not to be subject to surveillance and extensive policing.<sup>30</sup>

## ***(2) Why Does Technology Fail to Hold Policing Accountable?***

Technologically, policing accountability structures have depended on the visibility of the enforcement effort and the transparency of the regulatory modes that the technology employs.

### ***Visibility and transparency***

When policing is visible, we can publicly hold law enforcement accountable. Visible use of force often leads to public outcry when the policing effort is perceived as racist, brutal,

---

<sup>30</sup> In the context of the above-mentioned eBay discussion, *see*: Yuval Dror, *Supra* note 26. I expressed my view there: "The consent given in the user contract should be seen as 'coerced consent,' in the absence of any opportunity to exercise free choice, with no real alternative but to agree. This is most certainly not conscious consent." An insightful comment at Slashdot supported this argument and further developed it: "We are rapidly becoming a society in which corporations can strip individuals of their liberties not by virtue of law, but by using onerous contracts. Imagine if the utility companies forced a person to hand over keys to their residence when they signed up for service, so that the company could "inspect the premises in the interests of public safety". It wouldn't be long before the utility company would realize that they can make additional income by "renting" your key to law enforcement agencies on demand. But you, the resident would effectively have no say in this - you either agree to their terms, or you do without gas/electric/phone service. You see, the danger of this is that by "renting" the key, law enforcement no longer needs a warrant to search your house; you implicitly gave consent for entry to the utility company, who then resold that consent to law enforcement. It is these kinds of agreements which allow law enforcement to circumvent the checks and balances guaranteed by the constitution, and this is what makes them so dangerous. How long will it be before our lives and liberties are entirely beholden to corporate interests?"

non-proportional to the harm, or biased.<sup>31</sup> Visibility enables the suspect or bystanders to present their version or to record the course of action for later review.<sup>32</sup> Visibility further enables social mechanisms like reputation and shame to come into action and deter the law enforcer.

In addition, the transparency of the policing tool enables the understanding of methods of policing and the tracing of coercive force. Offline policing is to a large extent transparent. Moreover, the deterrent effect of the policing tool - the policeman's club, the check-point, and the handcuffs - is often tied to its transparency.

*Invisible Digital Cops* - Digital cops are invisible. In virtual space, policing often becomes invisible and the nature of force is no longer transparent. The user cannot tell most of the time that there is a policing tool in the environment. Policing tools operate in the background and are normally deployed at strategic information junctions outside the users' reach. Surveillance or information flow analysis are conducted when the information is on-the-fly or with duplicated copies of the information, leaving no trace or marks on the original documents. Moreover, policing functionalities are embedded within systems that also provide other functionalities and cannot be noticed. Even extremely intrusive tools, such as keystroke loggers installed on the user's computer, can be disguised to appear like innocent files attached to an e-mail. Tools which are designed to detect such software are regularly disabled to prevent disclosure.<sup>33</sup>

*Non-Transparent Policing* - The nature of the regulatory effect of the technology is not transparent. Technology can be visible and its installment can be publicly announced, yet we cannot immediately tell how it constrains our behavior. The technology is often

---

<sup>31</sup> For example we can recall the public reaction to Rodney's king brutal police beating; hot car pursuits for petty traffic violation; or the treatment of the protesters in the anti-war protest or anti-globalization rally.

<sup>32</sup> See for example the 1991 video cassette of the brutal beating of Rodney King, available at: <http://www.crimsonbird.com/history/rodneyking.htm>.

<sup>33</sup> The government, as reported, arranged with anti-virus software developers to adjust the software not to alert the existence of governmentally installed keystroke logger, "Magic Lantern" ("at least one antivirus software company, McAfee Corp., contacted the FBI ... to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a criminal suspect." (Associated Press report, cited at Wired News, "Lantern Backdoor Flag Rages" (November 27<sup>th</sup>, 2001).

installed as a black-box. Closed source software is transparent to the user in only a limited sense: he can observe the interface or the functional results of the process. However, he cannot tell how it operates and what additional features are embedded inside. Moreover, current legislation gives protection to security measures put in place to prevent users from accessing the code. At the same time, freedom of information legislation fails to supply the public with the right to observe the design or configuration of surveillance technology.<sup>34</sup> Courts have formerly only been willing to disclose the code of surveillance devices to a privileged few, based on the proposition that further disclosure will deem the technology ineffective and vulnerable to circumvention. Similarly, filtering tools which conduct core policing functionalities online are based on the premises that their black and white lists remain secret.

### ***(3) Why Does the Institutional Structure Fail to Hold Policing Accountable?***

Institutionally, inter-organization and intra-organizational operational structures serve to increase individual and organizational accountability. Hierarchy within organizations, operational walls between departments, and necessary collaborations open actions and inactions for review.

*Internal Institutional Design* - The internal organization of law enforcement was designed to foster an accountability culture with joint responsibility for actions and inactions. Service hierarchy supplies a chain of reports along the pipe. Internal procedures were set in place to obligate officers to subject their work to supervision and to bind the supervisor with the work of the supervisee. These notions are also reflected in requirements for approval from higher ranking officers for certain investigation techniques such as wiretapping. This creates a bi-directional accountability structure. Furthermore, by introducing the court to the initial stage, compliance with the internal prior authorization requirements is assured.<sup>35</sup>

---

<sup>34</sup> For a general discussion on the tendency to increase the secrecy of enforcement tools, *see*: Marc Rotenberg, "Privacy and Secrecy After September 11", 86 Minn. L. Rev. 1115 (2002).

<sup>35</sup> Requiring the court to authorize the operation we enjoy the court's accountability as an additional safeguard. Since the court's proceedings are publicly open to review, the court hesitates to function as a mere rubber stamp to enforcement requests and to face criticism.

This internal accountability structure is questionable when the policing shifts to a preventive mode, when technology enables acquiring the same information under reduced procedural requirements or when transferred voluntarily by third parties. Moreover, technology also serves to change hierarchal structures of command which have embedded monitoring and control into flattened structures of operation withstanding less internal review.

*Operational Walls* - Operational walls can also impose restraints on governmental power. Institutional operation walls were traditionally erected to separate law enforcement from intelligence and to control information sharing between governmental bodies. The emerging policing model blurs the institutional lines, embraces joint operations and facilitates information sharing practices. Newly enacted legislation in the current political climate is likely to further develop according to this trend.

*Inevitable Collaborations*- When certain operational needs require the police to collaborate in law enforcement operation with other entities (public or private), it expose the police to review and expose its operation to disclosure by the collaborator, whistleblowers or external inquiry of the links.

Technological tools incorporate skills and resources which traditionally resided in different institutions and enable law enforcers to refrain from forming collaborations which once seemed unavoidable. Technology enables the evasion of the accountability effect of collaboration.

Summarizing the argument thus far: When the legal, technological and institutional settings were changed, the policing accountability measures became easily circumvented, mute or non-functional.

This paper now turns to investigate the designs necessary for the new restraints which will come with power. It is crucial that we understand how policing functions in this environment in order to design the accountability guarantees to fit the new model.

But before we continue to inquire deeper into the structure of accountability for the new policing model, it would be instructive to take a closer look at the concept of accountability.

### **III. Accountability Online**

#### **A) Accountability – What For?**

Accountability as I see it, is defined as answerability. Accountability mechanisms are the processes, technologies, design principles and institutional structures which hold an entity to account for its actions and inactions.<sup>36</sup>

In the context of policing, accountability mechanisms can take various forms: a legal requirement to report the use of surveillance technology in investigation; a requirement to notify the subject of a search; a procedure to produce evidence in open court to support prosecution; a technological feature that reports to the subject of information when the information is accessed.

Accountability mechanisms assure answerability; they monitor compliance with substantive and procedural requirements and enable dynamic questioning of their ongoing efficiency and desirability. They deter the law enforcer from uncontrolled unilateral acts or abuse of power. Accountability mechanisms open a dialogue between the law enforcer and its relevant supervisor or community. They function as a counterforce to authority and tame unbridled power.

Accountability measures protect civil liberties. They assure that the democratically determined balancing point between security needs and civil liberties is observed. They expose infringements of civil liberties which are hidden in the practical operation of policing. They reveal the gap between a declared right and its fulfillment: They serve as a watch guard against unauthorized invasion of privacy. They expose inequality and discrimination which are hidden in policing practices. They protect one's right to speak freely by requiring a censorial power to answer for the unauthorized act of blocking or disruption.

---

<sup>36</sup> For further discussion on the notion of accountability, *see*: Jerry L. Mashaw, *Supra*.

Accountability is essential for more than protecting rights. Accountability promotes efficiency while enabling the measurement and assessment of performance. It forces judgment on the wisdom and fairness of decisions taken. It controls abuse and misuse while revealing the unauthorized use of power. In the context of law enforcement, accountability enables the security of the endeavor of enforcement itself. It acts as a tool to monitor against potentially insecure policing systems or a potential counter-intelligence effort.

### ***Accountability - More than Transparency***

Accountability is often mistaken as being synonymous with transparency. It is not. Transparency does overlap with accountability and does often serve the same goal. Accountability mechanisms, however, can function without being transparent. When a configurable network sniffer like Carnivore, for example, is set to limit the filtering of traffic only to documents which contain certain keywords and audits the configuration, it holds the law enforcer accountable. The operation need not be transparent and the deployment or the results of its operation are likely to remain concealed. Moreover, transparency might sometimes act in contradiction to the interest of accountability. When the parameters of operation are transparent, routing around the safeguards is encouraged. For example, in a situation when cameras are randomly deployed in investigation rooms to monitor the conduct of investigators: the transparency of those cameras which are live and analyzed allows the investigator to simply conduct the unauthorized practices in the unmonitored zones.<sup>37</sup>

### ***How does an Accountability System work?***

This paper takes a close look at how accountability systems operate. Accountability systems consist of the aggregated measures which function in relation to a certain entity or certain activity. Accountability measures can be embedded in different layers: the technology, the legal regulation, the institutional organization or the social construct.

---

<sup>37</sup> For further discussion on invisibility and disciplining measures' efficiency, *see*: Michel Foucault, *Discipline & Punish – The Birth of the Prison* (Vintage Books, 1995), “Panopticism” (p. 195- 228); Jeremy Bentham, *Postscript to the Panopticon*, in: *Jeremy Bentham, The Panopticon Writings* (Ed. Miran Bozoric (London, Verso, 1995), P. 29-95.

Accountability systems should be understood as a delicate puzzle in which each layer is assigned a certain role and operates and reacts to measures of accountability in other layers. Some accountability measures can be seen as supplementary to each other; some can be seen as redundant to assure survivability of the system if one measure fails to operate properly. The accountability effect is the overall out come of the functioning of all elements. Accountability is a dynamic construct, and tuning or distortion of one measure may have a domino effect on the functionality of others. Furthermore, accountability systems can normally adjust to the relative weakness of one layer by adding more strength to another layer. When the institutional structure of policing, for example, is relatively ineffective in holding the enforcer accountable, a tighter judicial overview at the legal layer balances the effect. Yet, when a certain layer is completely disabled or easily circumvented, the system might fail to regain balance.

### **B) The accountability Dynamic Equilibrium – User - Law Enforcement - Third Parties**

Accountability is a relational concept. The answerability of one entity for certain activity is always in relation to the entity to whom it should answer. One may be held accountable in relation to one entity but not in relation to another. Moreover, in interactive multi-party relations, accountability is a multi-dimensional concept which reflects the level of accountability appropriate to each entity vis-à-vis the other entities. Accountability in interactive relations should therefore be understood in terms of a point of equilibrium. Changing the measures of accountability which operates on one entity affects the overall equilibrium.

In the law enforcement context, the accountability of the individual interacts with the accountability of the law enforcer. For example: in the contemporary discussion of the “Accountable Net”,<sup>38</sup> many suggestions relate to the accountable user, who will be required to sustain a consistent identity over time by using a unique digital certifier. This measure which holds the user more accountable tends to erode the enforcer’s

---

<sup>38</sup> For the discussion about the accountable internet, *see*: Esther Dyson, “The Accountable Net”, New York Times, November 24, 2003; David Johnson, Susan Crawford and John G. Palfrey Jr., “The Accountable Internet” (Submission to the workshop on Internet governance by John Palfrey, February 26-27, 2004).

accountability. If the enforcer was normally required to be answerable for the reasons invoked to unveil the user's identity (so to attribute behaviors to this identity), now the technology does it automatically for the enforcer who can then potentially chase the user without undergoing inquiry.

Furthermore, in a multi-party enforcement environment, the accountability of additional parties interacts with both the user's and enforcer's accountability. When third parties are introduced to the equation, they can change the dynamic. For example: if a website owner is allowed to collect data on its users and enjoys the discretion as to whether or not to secretly share the information with the government, governmental accountability is affected vis-à-vis the user. The government can acquire data on users without undergoing judicial review of its information collection practices, without justifying the need and proportionality of its acts and without facing the user's objection upon notification of investigation.

To the contrary, when a third party enables the user to erode his accountability, as anonymization services enable users to evade traceability, it affects the accountability dynamic in a reverse manner.

In an environment where third parties are omnipresent and technologically required, their effect becomes a dominant factor in the dynamic accountability equilibrium.

### ***Accountability Arbitrage***

A common phenomenon in the online environment is Accountability Arbitrage.

Accountability is conceived as a cost to operation which rationale parties try to reduce, if possible. When a certain outcome can be reached in various methods but the accountability implications are different, we may expect the chosen method to be the one with the least accountability measures. Therefore, when the government can either collect information about a citizen directly and face the burden of proving its justification in a judicial process or alternatively query a commercial database which already collected the same information in a commercial context, the latter scenario is more likely.

Accountability arbitrage enables an entity which is subject to a certain accountability standard to reduce its level of accountability.

### ***Relational Accountability as Normative Continuum***

We should think of accountability not as a binary condition, but as a continuum. We should set the level of accountability at the point along this continuum which best serves our values. In this continuum, the levels of police accountability, user's accountability and third parties' accountability represent normative choices about the balance between liberty and security in society.

### ***Do Unaccountable Users Require Unaccountable Policing?***

The lack of user's accountability online is commonly used as a justification for the new policing environment. The erosion of policing accountability is commonly justified as a necessity in order to address the lack of users' accountability online. As claimed, users escape accountability online by not being traceable so that we cannot attribute online activities to real-world identity. It is further claimed that by acting outside the jurisdiction individuals can escape local accountability. Therefore, it is concluded, we need to enable the government more leeway in handling these new types of unaccountable criminals and relax accountability requirements which we impose on policing. The logic is simple: to properly react to the diminishing level of users' accountability, we need to allow reduced governmental accountability.

This paper claims that the above mentioned approach is mistaken.

The solution for diminishing level of users' accountability will arise from creative thoughts about how to reconstruct users' accountability in a manner that co-exists with governmental accountability. Yes, we should design users' accountability. Yet, we need to be aware of imposing too much of an accountability burden on the user, which alters the balance between policing power and liberty. I argue that instead of justifying one erosion in accountability by another and lowering accountability standards altogether, we

ought to redesign accountability for both the user and the law enforcer by mutually raising the bar.

### ***Toward an Accountable User – “Traceable Anonymity”***

I agree with the factual claim that a user’s accountability is potentially eroded online. The features of the environment enable the user to remain untraceable, as the core internet protocol was not designed with security in mind. However, with the existing internet protocol and without changing the architecture of the information environment, we can establish a system of user’s accountability which is based on potential traceability and message attribution.

A users’ accountability system has to take into account five functional goals: (I) identification of the user, (II) traceability of the origin of the message, (III) integrity (unity) of the message, (IV) readability of the message, and (V) retention of evidence for judicial proceedings. Any model of user’s accountability presents different normative choices about the balance between law enforcement interests, individual privacy, anonymity and freedom of speech on the Internet.

Elsewhere, I have proposed a “Traceable Anonymity” model which offers to create the appropriate balance. Based on existing PKI encryption infrastructure, this model draws the institutional and architectural foundations of a users’ accountability system. This model aims to maintain the users’ ability to use the Internet anonymously and without their actions being recorded, but at the same time enables law enforcement agencies worldwide, subject to a judicial decision, to trace the identity of a user who misuses anonymity to commit a crime. Under this model, any electronic message is signed with a digital signature using a unique private key that is issued to the user after an identification process by a private and regulated certificate authority. A digital certificate that is attached to the message does not reveal personally identifying information<sup>39</sup> but assures

---

<sup>39</sup> The digital certificate does not include a constant serial number, and therefore prevents systematic monitoring of the identity which correlates with the digital certificate.

that an identification process<sup>40</sup> was conducted.<sup>41</sup> If the user misuses his anonymity to commit a crime, the court (local or international) may order, with attendant due process protections, the certificate authority to disclose the user's identity<sup>42</sup>. The revealed information links the identified user to the specific crime, but to no other activity, and the digitally signed message serves as evidence of the criminal act. This system would be technologically scalable to the international level and can be used as an efficient mechanism to enable transnational law enforcement efforts. At the same time, the system could accommodate cultural differences and restrain coercive unilateral abuse of the system, by regulating the conditions under which a certifying authority follows a foreign order to reveal the user's identity.

The technological and institutional details of this model are discussed elsewhere (and presented in this conference in the IJCLP panel on "International perspectives on Internet and Communications Regulation"), yet the idea is simple. The "Identified Anonymity" Model ties the accountability of the user to the accountability of the police. It increases the users' accountability from the current level by making users potentially traceable. Yet it prevents the government from unveiling users' information unless it justifies the need before an independent judicial body. Even then it can not trace or attribute other actions of the user. The certifying authority serves to help the identification process, but cannot access its own database without judicial order, as the court holds half of the key to the database. This also prevents a tyrannical regime from accessing the database unilaterally.

---

<sup>40</sup> On the possibility of identification architecture which supports individual's choice about how much information to reveal, *see*: Lawrence Lessig, "Code is Law – on Liberty in CyberSpace", Harvard Magazine, January – February 2000.

<sup>41</sup> Once the certifying authority identifies the holder of the signature device which correlates with the digital certificate, it saves the identifying information and the software automatically encrypts the information on its database. From this stage, the certifying authority can not access its own database, as half of the key to the database is held by the court. This measure protects the information from potential abuse by the private certified authority.

<sup>42</sup> It is important to clarify that the proposed technology enables direct identification when we return to the certifying authority, but it prevents a "weak link" along the chain of communication from unilateral act to unveil the user's identity. Currently, users are exposed to unilateral decisions by the ISPs (or other player on the communication route) to disclose their identity.

In conclusion, we should not justify the lack of policing accountability as a response to the decrease in the users' accountability. We ought to instead construct an appropriate policing accountability system.

## IV. Designing for Accountable Online Policing

### A) Design Guidelines for Accountable Policing

Now that the nature of policing accountability and its interaction with the accountability of other parties in the environment has been examined, we can set the guidelines for designing a policing structure which serves both efficiency and liberty.

The following concepts should serve as foundations for the design of the accountability system:

***Optimal Equilibrium*** - We should stop the race to the bottom towards diminishing accountability of all relevant parties - individuals, law enforcement and third parties. We should aim to raise the multi-dimensional equilibrium point to the optimal level. When we design the system, we should think of the full matrix of accountability and consider dynamically the correlating effect of changes in accountability mechanisms which restrain a certain party on the accountability of other parties.

***Liberal Accountability Values*** - Accountability requirements should correspond with our liberal democratic notions. These notions require different levels of accountability assigned to different parties. Based on these liberal notions, the individual ought to be held accountable only to the minimal level necessary to enable a viable security model. In this regard, an increase in the level of individual accountability should have to withstand harsh scrutiny. At the same time, holding policing accountable should be at the highest optimal level possible in order to control the use of policing power while simultaneously enabling efficient operation.<sup>43</sup>

---

<sup>43</sup> This introduces important questions about over-accountability. Can we have too much of policing accountability? Does accountability at a certain stage become an obstacle to effective policing? When does policing accountability erode individual accountability?

My notion of accountability is flexible enough to prevent the problem of over-accountability. I acknowledge in my concept of accountability the relational nature of accountability and its potential tension with transparency. Therefore, when we design accountability measures we also have to consider whether it might lead to an erosion of accountability of other players and whether the accountability measures require making the technology fully transparent. Relative concepts of transparency and selective

***Medium Sensitivity*** –When we design the mechanisms for users’ accountability, third parties’ accountability or law enforcement’s accountability, we need to be sensitive to the effect on the medium.<sup>44</sup> A structure of accountability which affects the architecture also affects the political structure of the information ecosystem. The design of the accountability structure for the communication network influences the relative powers in the public discourse and affects the nature of the discourse.<sup>45</sup> An accountability structure for a communication network has to consider these political implications of its implementation.

***Circumvention Analysis*** - At the design stage, we should simulate the possible circumventions of the set mechanism and, if required, establish mechanisms to monitor or prevent them.

***Functional Equivalency*** - We need to establish the principle of Functional Equivalency in order to impose comparable accountability standards on similar policing actions to prevent the above-mentioned accountability arbitrage.

***Layers of Accountability*** - We need to consider the functionality of all layers of accountability - legal, institutional, technological and social - working in tandem. We need to see how to design the layers to supplement and support each other rather than contradict each other. We need to explore opportunities of synergetic effects across layers. Simultaneously, we should normatively evaluate the trade-offs when using one layer rather than another.

***Continuum of Accountability*** - We should, if possible, create flexible accountability measures that can be adjusted to changing circumstances. The flexibility will enable

---

exposure to review can most of the time solve the problem of over accountability. I further address these questions in the elaborated version of this paper.

<sup>44</sup> The discussion on information service provider’s liability demonstrates this claim. In order to enjoy the benefits of a robust, unmonitored, and open environment, the legislator refrains from imposing liability on service providers for third parties’ content.

<sup>45</sup> It dictates who controls the flow of information in society, who has the ability to squelch other voices, whose voice will be amplified and whose voice will be silenced. The design also determines the ability of the government to control the flow of information and to block certain information or certain speakers. On the political economy of the information ecosystem, see: Yochai Benkler, “Siren Songs and Amish Children: Autonomy, Information, and Law”, 76 N.Y.U. L. Rev. 23 (2001).

keeping a mechanism in operation even if special needs require a reduced level of accountability (e.g. terror investigation). The design has a continuum mode of operation in mind, rather than a binary mode which makes possible only enabling or disabling an accountability measure.

## **B) Design towards an Improved Accountability for the New Policing Model**

Having established a set of guidelines for design, we should think through the new accountability mechanisms in greater detail. New technologies can lead to improved and innovative legal and institutional mechanisms of accountability. The development of new technology is a window of opportunity to design accountability mechanisms which fit the new environment.

### ***(1) Technology Facilitates New Supervising Institutions***

Technological measures can support the establishment of new institutions for the supervision of policing. Technology interplays with institutions in society. Technological developments render certain institutions ineffective or relatively weak.<sup>46</sup> Other technological developments can set the groundwork for the establishment of new institutions to supply services which were sub-optimally provided before. Technological developments currently enable setting internal, inter-organization and external supervising bodies to hold policing accountable. The policing accountability deficit can be corrected if we design policing tools to facilitate supervision. To fully understand this claim, we shall start by introducing the technological accountability measures.

Imagine the following features embedded in “Total Documentation” tools used by law enforcers: A tamper-proof log audits the time/ date of collection of any piece of information which enters the digital investigation folder; another log audits the access to digital evidence examined by the investigator and the queries run on the investigation databases; all communication data (traffic data) to and from the law enforcer is retained and visualized to demonstrate the enforcement networks of operation and the sources of

---

<sup>46</sup> For example: central censorial authorities which were based on concentrated media technology were deemed relatively inefficient with the shift to distributed information ecosystem on the Internet.

information obtained; e-mail and telephone calls made by the investigator are recorded and stored on digital media and can be analyzed with natural language search tools; patterns analysis tools look for suspicious access to information or abnormal investigation process.

The imagined “Total Documentation” scenario may sound familiar, as it is no different from practices in many corporations to monitor their employees’ work, to assure compliance with work procedures, and to protect from fraud, abuse and potential liability.<sup>47</sup> Employing these technologies will enable establishing the institutions needed to supervise the policing operation. The main obstacles to efficient supervision have always been resources and information. Technology reduces the costs dramatically and enables the remote supervision of full police operation.

Current technology is flexible enough to facilitate the establishment of various institutions to fulfill various supervision functions. It can produce accounts which are specifically tailored to each supervisory institution and can measure and review different aspects of the policing operation. We can imagine the supervising bodies getting selective access to the different layers of the accounts and produce distinctive reports based on their position, needs and authority. The review can respect existing classification and can allow access to investigation information without revealing personally identifying information. It enables the supervision of the work of individual policeman to prevent abuse of power. It can enable the aggregate analysis of the policing operation to identify patterns of crime and enforcement, such as racial profiling and actual enforcement prioritization.

## ***(2) Technology Facilitates New Legal Accountability Regime***

Technological features can also support the establishment of new legal accountability mechanisms. Value-driven design of technology may enable the construction of legal procedures that are better equipped to hold policing accountable.

---

<sup>47</sup> Claims departments in insurance company, for example, employ such tools to monitor the work of their claims investigators.

### *Towards an Accountable Search and Seizure Law*

Technology enables us to redesign search and seizure law to hold the government to a higher standard of accountability.<sup>48</sup> Currently, in an ex-parte procedure the court issues search warrants which give wide authorization to law enforcement to search in the designated premises for all documents and peripherals for incriminating evidence. Why? Because ex-ante the court has no information on which to base a decision to limit the search to certain files or to predict where the information can be located. Standard warrants which are daily issued fail therefore to genuinely meet the particularization and minimization requirements.<sup>49</sup> In practice, law enforcers hardly ever conduct searches on-site. The officers on-site copy the hard discs and other information found on storage devices and hand the copies for deferred experts' thorough search. The initial warrant enables law enforcement to conduct such a thorough search with minimal interference and with no audited process. Only when the search reveals new evidence which seems to exceed the originally investigated crime covered by the warrant, do the police return to court to obtain an additional warrant. At this stage when the incriminating evidence is known to the police, the court procedure is a mere rubber stamp.

The reality, as described above, reveals that searches are conducted in a troubling procedure which potentially strips computer users of all their privacy expectations in their most intimate files even for a preliminary investigation of a petty crime. While in physical searches, the suspect's presence in the scene enables a two-sided story of the process to deter the government from abusing the warrant for external goals or exceeding their authorization - no such mechanisms operate in the digital search. The court has to rely on the law enforcement's version of how the search was conducted, which is susceptible to the "manufacture" ex-post of a search process which abides by the legal requirements.<sup>50</sup>

---

<sup>48</sup> See in details: Nimrod Kozlovski, *The Computer and the Legal Proceedings – Electronic Evidence and Court Procedure* (Israeli Bar Association, 2000) (Hebrew) p. 50-109.

<sup>49</sup> This procedure is justified by scholars as a necessary evil since suspects can save files in misleading names, hide them in unexpected folders or scramble the content to appear innocent.

<sup>50</sup> In digitized evidence it is relatively easy for the law enforcer to introduce in court alternative evidence to the one which might present legality concern. It is analogous to reverse engineering for law enforcement, in

Can search and seizure law be more accountable? Most definitely, by changing the sequence to seizure and then search and introducing new authorization procedure and auditing requirements. The court can authorize first the seizure of the relevant information. In a simple and cheap mirror copying process, a copy of the information is secured with law enforcement and detached from the suspect's control. At this stage, we can structure various alternative procedures for search authorization which assure better accountability: The court can appoint an expert as an officer of the court to examine the seized data before the police observe it. The expert's input can support the court's decision whether or not there is ground to issue a warrant based on law enforcement's claims and under what restricting terms. Alternatively, we can enable an adversary process in which the owner of the information, other users of the computer or the suspect can raise objections to the search or to its scope. After all, when the surprise element which was essential to physical searches is no longer required as the evidence is safe with law enforcement, why not enable a fair process that truly reports one's right against intrusive invasion to his intimate realm?<sup>51</sup>

Alternatively, we can allow law enforcement to conduct the search on the seized information without further procedure but require using a tamper-proof and copy-protected copy of the seized information with an audit log for all queries and access to files. Audited searches will enable the court and the defendant in an event of prosecution to review the actual practice of the search and to question the sequence of investigation.

### *Towards an Improved Judicial Review*

Furthermore, in the current system we have no meaningful judicial review of the legal execution of wiretap orders and search warrants if law enforcement decides not to file for prosecution. Law enforcement can exceed the authorization of the warrant, but undergo no accountability by refraining from prosecution. This conflicts with a core principle of

---

which the law enforcer is already familiar with the evidence, and reverses the process of production to enable an alternative production path which will not face the same legality concerns. Since retrieval tools can easily track a file once its content and format are known, it requires no special effort after the evidence is known to "manufacture" a legal process of acquisition.

<sup>51</sup> This rationale informed in England the design of a special civil search procedure for computers within the process of Anton Pillar warrants, *see*: Nimrod Kozlovski, *The Computer and the Legal*, *Supra* note 48, p. 110-124.

the legal system that court orders are accompanied with a mechanism to supervise their execution. Normally the existence of an opponent or other interested party suffices to assure supervision, and in their absence the court in many legal systems is authorized to appoint an officer of the court to supervise the execution of the order. To assure accountability in execution of wiretap orders and search warrants, we can design a process which requires law enforcement to report back to court after execution. We can further employ the above-mentioned technology to supply the court with objective information about the execution to enable a semi-judicial process of review. Moreover, such a process is essential, as more searches are conducted remotely and without notification (or deferred notification), while the once exceptional sneak and pick searches gradually become the norm.

### ***(3) Holding Private Policing Accountable***

We should further increase policing accountability by targeting the partnership between the government and private parties and regulating private enforcement. Within the limited scope of this paper, I will just mention a few possible venues of regulation.

*Agency Rules* - Within public law, the court should redraft agency rules to cover the practical partnership practices and the delegations of power which utilize private parties for core law enforcement assignment. The doctrine should regain its original rationale and question whether private parties are de-facto employed for governmental actions. The doctrine should divert from the current narrow application, which recently, in the *Jarreet* case,<sup>52</sup> failed to regulate even the extreme case of intentional encouragement of a hacker to illegally hack for policing purposes.

*Liability and Openness* - We need to regulate to amend the current “deal of partnership” which reduces both the police’s and third parties’ accountability. The current mode of public-private partnership replaces liability and openness with immunity and secrecy and

---

<sup>52</sup> *U.S. v. Jarrett*, 338 F.3d 339 (4th Cir. 2003). In this case the court decided the although hacker had help the government in the past in a pornography case, and the government in a series of e-mails praised the hacker for his efforts and assured that he would not be prosecuted for his actions, the exchanges were insufficient to create an agency relationships.

acts in contrary to rooted foundations of the legal system. The Freedom of Information Act should open for review the information which is handed to the government while preserving the trade secrets interests exception only when necessary, by anonymization of the data. This should be supported by civil liability for negligent handling of information which causes harm to the individual.

*Consented Search* - We should question the Third Parties Consent doctrine which practically treats all information observable by third parties as information whose subject assumes the risk of disclosure to the government. In an environment in which third parties are omnipresent and technologically required, there is no meaningful choice to the individual whether to share the information with third parties or not. The doctrine has to reflect it.

*Fair Information Practices* - We need to enact Fair Information Practices which are common in comparative law and assure the accountability of the data collection and handling stages. This will further empower the subject of information to control accuracy and up-to-date amendment of information, contextual integrity and secondary use of information.

### **Concluding Remarks**

The new information environment empowers us, yet simultaneously introduces unexpected vulnerabilities. To address these vulnerabilities, law enforcement is rethinking its model of operation. The emerging model of law enforcement is relatively efficient in addressing the new challenges, but creates an unchecked policing power. It is now the time to introduce accountability into the policing model.

In “Inherit the Wind”, the movie based on the Scopes “Monkey Trial”, the character playing the famed litigator Clarence Darrow declares:

“Progress has never been a bargain. You've got to pay for it. Sometimes I think there's a man behind a counter who

says, 'All right, you can have a telephone, but you'll have to give up privacy and the charm of distance...''<sup>53</sup>

In this paper I respond to Darrow's skeptic. I aim to prove that indeed progress can be a "bargain". We can have progress with civil liberties. We can enjoy the benefits of information technologies without paying the price.

We can benefit from a secure online environment which is policed by accountable law enforcement. A window of opportunity is currently opening for designing the technology, the institutions and the legal framework that will work in concert to enhance accountability.

---

<sup>53</sup> *Inherent the Wind*, 1960, directed by: Stanley Kramer.