Surveillance & Society

Opinion

A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics

Gary T. Marx

MIT, United States. mailto:gtmarx@mit.edu

Introduction

> It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application resolve.
>
> Edgar Allen Poe, *The Gold Bug*

The title of this article refers to efforts to defeat the polygraph by stepping on a tack hidden in one's shoe. This does not work when subjects are told to remove their shoes.

A tack in the shoe is an example of an individual instrumental *neutralization* technique. The requirement to remove shoes is a *counter-neutralization* technique. In this article I suggest some concepts to help order an array of behaviors and attitudes in opposition to, or in support of, surveillance. Behavioral neutralization is a form of resistance.[1]

The rhetorical claims for a tool offered by surveillance entrepreneurs must be tempered by empirical analysis of actual capabilities and consequences. Statements about the potential for good or harm (in the case of anti-surveillance entrepreneurs) need to be documented, not simply asserted.

With respect to the views of many readers of this journal alert to dystopic outcomes, it is well to note that just because something negative could happen, does not mean that it must happen. We need to consider factors tending toward or away from such outcomes. One factor working against such outcomes is resistance by surveillance subjects. Given the neglect of this topic, this edited volume is most welcome.

The advantages of technological and other strategic surveillance developments may be limited and success (if present) short-lived --the same holds for new developments to defeat surveillance.

New technologies rarely enter passive environments of total inequality. Instead, they become enmeshed in complex, pre-existing systems (often with weak heels and flies circling the ointment). They are as likely

[1] This contrasts with the original meaning of neutralization within sociology (Sykes and Matza 1957) which involved attitudes thought to lead rule breaking, not the behaviour itself. In the case of resistance to surveillance, however, the frame of reference is less clear for defining legitimacy. Some cases of neutralization are moral (and legal) violations just as some cases of surveillance are. The consistency between attitudes and behavior may be weaker in surveillance contexts than in many other settings.

Marx, Gary T. 2009. A Tack in the Shoe and Taking Off the Shoe: Neutralization and Counter-neutralization Dynamics. *Surveillance & Society*, *6*(3): 294-306.
http://www.surveillance-and-society.org | ISSN: 1477-7487

to be altered as to alter. Professional associations, oversight organizations, and political and social movements affect this, as do the new markets that control technologies create for counter-technologies.

Many factors inhibit the full unleashing of surveillance: logistical and economic limits, competing values, the interpretive and contextual nature of human situations, system complexity and interconnectedness and the vulnerability of those engaged in surveillance to be compromised. Particularly in liberal democratic societies, there is space for resistance, irony and surprise.[2]

Surveillance needs to be viewed as a dynamic process involving emergent interaction and developments over time with respect to *anti- a*nd *pro-surveillance* actions. A natural history model is required. Such an approach involves a series of logically and temporally linked, yet distinct activities called *surveillance strips* that occur within a broad field. These are creation; adoption; data collection (including the behavior of subjects as well as of agents); analysis and interpretation; application; and fate of the data (and eventually the tactic). Viewed sequentially these represent the life history of a *surveillance occasion.*

Resistance and support may be studied in many empirical and analytical places and take many forms. They can be viewed in relation to the stages of surveillance occasions noted in the preceding paragraph. They may be directed at a specific application or at the tactic more broadly. Efforts may be instrumental or non-instrumental.

Non-instrumental forms of resistance can be seen in the sheer contrariness to authority that Foucault (1977) writes of regarding, “a certain decisive will not to be governed.”[3] Scott’s (1985) work on the symbolic and/or non-instrumental expressions of indignation and rebellion are related. The contumacious need not be strategic.

Neutralization may be direct or indirect. It may seek to effect the data offered (or taken from) the subject, the identity or location of the subject, the conditions under which data collection occurs, or it may directly engage the instruments of data collection and analysis. It may involve the intersection of the body and technology or the non-organic.[4]

Resistance may involve a subject acting alone, or an interest group or social movement acting in cohort. As Martin, van Brakel and Bernhard (this issue) argue much resistance to, and support for, surveillance goes beyond the more easily seen subject-agent relationships.

Individual responses may be collective in the sense that many persons respond the same way to the same stimulus, however, they need not be organizationally inspired or coordinated. Yet they may be linked as when protest movements grow out of, or encourage, individual resistance and provide education, models, resources and legitimation. The hydra-headed decentralized features of computing (e.g., the virtual advocacy networks for publicizing surveillance practices identified by Gibbons and Introna (this issue) suggest an intermediate form.

The spread of the new surveillance has been accompanied by organized political and legal challenges from established civil liberties, consumer and worker organizations as well as by new organizations.[5] The

[2] For example consider case studies of welfare surveillance and drug testing (Gillom 2001 and Moore and Haggerty 2001).

[3] Folklore suggests that the United States, France and Italy may stand out in that regard relative to England, Canada and Germany.

[4] In considering biometric surveillance Ball (2005) notes resistance strategies to interrupt the flow of information from the body, and to alter the timing and codings of the body.

[5] Consider the awareness-raising and lobbying of new organizations such as the Electronic Privacy Information Center and Electronic Frontier Foundation, the Center for Democracy and Technology, Computer Professionals for Social Responsibility, the

politics of surveillance can even involve one level of government resisting another.[6] For these challenges the emphasis is on stopping or regulating a broad strategy or a particular tactic within it, not a given application.

Resistance and support can also be seen in cultural efforts by advocacy groups to educate the public, create awareness and offer alternative sources of data and interpretation. This may be general or directed at a particular action.[7] Consider the guerrilla theatre presentations of the New York surveillance players, artists and satirical and critical offerings on the Internet.[8]

While all of the above resistance activities fit within a broad *anti-surveillance* tent, here I emphasize individual instrumental responses in the data collection stage. One approach to this descriptively considers all the neutralization means for a given tool (e.g., drug testing, the polygraph, red light cameras).[9] While this may help those disrespectful of the powers that be, it does little to increase understanding across cases. A more analytic approach looks beyond specific applications for general reoccurring forms.

There are a limited number of repertories of *surveillance neutralization* and *counter-neutralization*, even though the specifics and settings vary greatly. This limit reflects the directive power of culture and commonalities in the nature and structure of surveillance contexts. There are parallels to Charles Tilly's (1995) work on *repertoires of contention*.

I will discuss techniques of *neutralization* subjects adopt, the *counter-neutralization* of agents and subsequent subject *counter-counter neutralization* responses. These are inductively drawn from the empirical record. Given the open-ended nature of the process this list could be continually extended.

The neutralizing actions treated here involve direct resistance or avoidance rather than a broad strategic response such as challenging a law or encouraging a boycott. The resistance actions taken by an individual to defeat a given application are often covert in order to maximize effectiveness and/or to avoid suspicion and sanctioning. The goal is to defeat a given use not to abolish its use.

Privacy Rights Clearing House, the Privacy Foundation (University of Denver), Privacy International, Statewatch.org and traditional organizations such as the American Civil Liberties Union (in particular its project on Technology and Liberty) and Consumers Union (and more specifically here Adbusters and CASPIAN (Consumers Against Supermarket Privacy Invasion).
There are also groups with specific concerns such as the National Rifle Association regarding gun sales and ownership, the National Abortion Rights Action League regarding reporting requirements for abortions by minors, and universities concerned over reporting and monitoring requirements for foreign students. There are also of course many industry groups active in lobbying and in offering communications about the topic such as the U.S. Chamber of Commerce concerns over work monitoring and the Direct Marketing Association's interest in third party commercial uses of computer data.

[6] Thus in Japan after the launching of a controversial national identification number some cities cooperated with the national government, some such as Yokohama gave citizens a choice of whether to allow their data to be entered into the system and some cities refused to cooperate. (Murakami et al 2007) In the U.S. following passage of the Real Id Act of 2005 imposing federal standards for driver's licenses, a number of states indicated they would not cooperate. During the civil rights movement in Alabama the NAACP refused to turn over its membership lists to the state, a decision later upheld by the Supreme Court [(NAACP v. Patterson, 357 U.S. 449 (1958)]

[7] Relatively little is known about the beliefs that accompany general attitudes of support or opposition to current practices. Wells and Wills (this issue) offer an example in their work on resistance narratives with respect to speed cameras. Subject's concerns involved doubts about validity, applying the tactic to those seeing themselves as law abiding and better uses of the resources for more serious offenders.

[8] YouTube offers an abundance of materials on big brother and related themes. The ACLU's Pizza Palace surveillance clip is a classic (http://www.aclu.org/pizza/)

[9] For example we can note that self-testing, substitution of clean urine, flushing one's system, adding a distorting substance such as bleach to a sample, or accounting for a positive finding by reference to a medication taken are all *drug test* neutralization means. Or we can also consider these as examples of *generic forms* involving discovery, switching, distorting and explaining moves.

Twelve techniques of neutralization are discussed in detail in Marx (2003). Table 1 defines the types and Table 2 (below) offers illustrations from the workplace context. Equivalent examples can be shown for other contexts such as the marketplace, government and interpersonal relations.

***Table 1:* Twelve Neutralization Moves**

Move	Action
Discovering	Find out if surveillance is in operation, and if it is, where, by whom and how
Avoiding	Choose locations, times periods and means not subject to surveillance
Piggy backing	Accompany or be attached to a qualifying object
Switching	Transferring an authentic result to someone or thing it does not apply to
Distorting	Altering input such that a technically valid result appears but the inference drawn from it is invalid
Blocking	Eliminating or making data inaccessible
Masking	Involves blocking in that original information is shielded but goes beyond it to involve deception with respect to factors such as identity and location
Breaking	Rendering the surveillance device inoperable[10]
Refusing	"Just say no" – ignore the surveillance and what it is meant to deter
Explaining and contesting	Accounting for an unfavourable result by reframing it in an acceptable way or offering alternative data and the claims of rival experts, making rights claims
Cooperating	Collusive moves with agents
Counter- surveillance	Role reversal as subjects apply the tactics to agents taking advantage of the double edged potential of tools[11]

***Table 2:* Examples in the Workplace Context**

Neutralization Technique	Data Collection Context: Workplace
Discovering	Bug detectors
Avoiding	Choose employer that doesn't monitor electronic communication
Piggy backing	Walk into restricted facility behind person with access
Switching	Substitute clean urine sample
Distorting	Holding down computer keys to appear productive
Blocking	Encrypting communication
Masking	Using another person's id and password
Breaking	Add battery acid to a urine sample
Refusing	Don't file reports about dating another employee
Explaining	"I didn't know there was marijuana in the brownies"
Cooperating	Advance warning of drug test from supervisor
Counter- surveillance	Audio-recording harassing statements by supervisor

[10] A system can also be functionally broken by being flooded, although this is more likely to be a protest resource than a tactical neutralization action directed at data collection. Harassing calls intended to tie up phone lines or filing endless bureaucratic forms are traditional means of protest against organizations. More recently Kiss (forthcoming) identifies *overwhelming* as a text messaging protest tool used at the Republican National Committee meeting in New York. Police did not have the resources to immediately respond to the content of thousands of messages. This might also be seen as a kind of refusal, simply acting because it was believed control was not up to the task.

[11] Huey (forthcoming) emphasizes a different meaning of counter-surveillance in exploring how activists use freedom of information laws to learn about government actions. Activists tended to see their actions not as anti-surveillance (the term surveillance is viewed negatively through its association with covert behavior), but as involving democratic principles of accountability and transparency. Covert surveillance is to be stopped by political changes, not by mimicking what they are against or by more powerful technologies. This suggests a qualification to Simmel's observation that adversaries come to resemble each other in their use of tactics. For those motivated by high democratic principles the means they use may be as important as the ends. This is also involves the distinction between a given tactical means and a broader strategic effort to alter or stop its use.

Taking Off the Shoe: Neutralizing Neutralization and Beyond

> The observer, suspecting that what he might have treated as an unwitting move is actually or possibly an obfuscation or misrepresentation, suspecting that what appears to be ingenious in fact could be shot through and through with a gamesman's manipulation and design, suspecting this, he can attempt to crack, pierce, penetrate, and otherwise get behind the apparent facts in order to uncover the real ones. The observer performs an uncovering move.
>
> Erving Goffman, *Strategic Interaction*

The strategic actions of both watchers and the watched can be thought of as moves in a game, although unlike traditional games, the rules may not be equally binding on all players. The 12 moves above provoke counter responses such as the uncovering moves Goffman identifies. Agents serious about their work must eternally wonder if the reality they see is the reality it appears to be.

As the countless examples of neutralization suggest, human ingenuity is often richer than the possibilities that can be anticipated and built into the machine. In conflict settings the flexible and creative human spirit so far has some advantages over "dumb" machines with a limited number of programmed responses (at least the first time around). Yet machines are quick learners, just as some subjects are.

Neutralization is a dynamic adversarial social dance involving strategic moves and counter-moves. It has the quality of an endless chess game mixing old and new moves. Those in the surveillance business respond to neutralization efforts with their own innovations which are then responded to in a re-occurring pattern. Whether for agents or subjects, innovations may offer only temporary solutions.

The cat and the mouse continually learn from each other and reiteratively adjust their behavior in the face of new offensive and defensive means.[12] For example the Department of Defense through its Polygraph Institute offers a 40 hour course to prepare examiners to deter, detect and prevent polygraph countermeasures.

The quality of play might improve or become more sophisticated, but this is within a broad moving equilibrium in which advantages from an innovation are not constant, particularly over time. This is one reason why "the war on …" rhetoric, with the idea of final victory, is inapplicable to much domestic surveillance. A better military analogy lies in escalation and a kind of surveillance arms race captured by "the see-saw principle" of new developments balanced by counter-developments.

Several agent moves mirror those of subjects and equivalent tools may be used. Thus the uncovering moves noted by Goffman are examples of discovery. Cooperative moves with exchanges beneficial to both parties may be initiated by either party. But some distinct forms are also present. This results from the frequent power and other resource differences between agents and subjects and their divergent goals.

Some other major counter-neutralization moves are: technological developments, the creation of uncertainty through repetition, randomization and deception, the use of multiple means and the creation of new rules and penalties.

[12] Gillham and Noakes (2007) apply a reiterative perspective to protest groups and authorities. Fernandez (2008) provides a careful case study of Seattle. Oliver and Myers (2003) offer a theoretical analysis.

Table 3: **Four Counter-Neutralization Moves**

Technological enhancements
Creation of uncertainty through repetition, randomization and deception
Multiple means
New rules and penalties

Technological Enhancements

This reflects the traditional engineering model of relying on technical innovation. Consistent with the new surveillance argument, the counter-neutralization technologies (along of course with neutralization technologies) become more powerful, penetrating, broader in reach and “smarter”. They also have become softer, in some cases to intentionally by-pass the subject’s knowledge and consent. (Marx 2006)

Most drug tests now immediately take temperature readings –a reading less than 90 degrees is presumed to indicate dilution or substitution. Automated fingerprint access systems also now often have a temperature sensor. A “drugwipe” test claims to “pick-up where standard drug testing leaves off.” It identifies drug residue on a desktop or other items. Or, “after the workers have gone home,” a vacuum like device can be used on computer keyboards to “surreptitiously check for illegal drugs”.

X-ray machines can produce images of anything between a traveller’s clothing and skin, making it harder to hide items. X-rays may be used in traditional ways to look within the body e.g., in a search for swallowed balloons containing drugs.

The “electronic biological passport” required of cyclists adopted by the World Anti-Doping Agency and the Union Cycliste Internationale in 2008 offers a new approach to identifying dopers. (http://www.uci.ch/Modules/ENews/ENewsDetails.asp?id=NTQzOA)

Rather than the perennial, ever-changing direct search for new forms of doping and for substances to block discovery of this, this approach is indirect. It relies on a sequence of tests and statistical tools to create a unique profile of the individual that serves as a base line for assessment. This bypasses the difficult search for newly created banned substances that initially are often unknown.

Police have new tools to use for the pesky problem known in the trade as NCTR (non-cooperative target recognition). Multiple bands and laser radar (Lidar) are more difficult, or impossible, for speeder to discover. In giving an instantaneous reading of a car’s speed, the laser eliminates slowing down as an option. Another police tool called "the interceptor" is a detector detector. It emits an alarm and flashing red light when it identifies a car using a radar detector.

Some electronic tagging systems now use sound waves to trip the alarm. The waves penetrate metal enclosures such as metal-lined shopping bags that were previously used to defeat tagging systems. Improved means of fastening make it more difficult to remove electronic tags –whether from consumer items or those worn as anklets or bracelets.

Requiring school uniforms helps identify outsiders. Clothes without pockets and a requirement that shirts be tucked in (so it is harder to hide weapons) are advocated as ways of reducing school violence.

Paper, explosives, typewriters and printing presses, and more recently, computer printers and copy machines, may carry unseen identifiers. These can be seen as counter-neutralization means to a subject’s implicit avoidance in assuming anonymity.

Screening moves (which might also be called *front-end exclusionary moves)* seek to deny neutralizers the chance even to try. Bar code and other scanners are programmed to recall cancelled or suspect identities and patterns. Profiling and data bases are an effort to extend historical memories and avoid risks. The bad apples are to be stopped before they get into the barrel, even at a cost of excluding some good apples.

For the polygraph, piezoelectric sensor pads placed on the seat or armrests of a chair or under the subject's feet are used to identify physical countermeasures such as sphincter contracting.

Randomization, Repetition and Deception

These strategies seek to counter the opportunity structures for neutralization. Such opportunities can be related to the impossibility of continually scrutinizing everyone all of the time and to the strategic advantage that may come from observing predictable agent patterns. Surveillance may appear at unpredictable times, places and forms. The goal is to create uncertainty. The possibility of surprise is intended to deter, or if not, to lead to discovery. Trickery is used to pierce informational borders.

For both agents and subjects, as a customs official said, "when you do it all the time, it's predictable. If you have a predictable regimen, it can be exploited." The random application of surveillance can not be as easily "gamed". Consider the search of air travellers or those at borders based not on anything suspicious, but on a table of random numbers. Roving inspections on subways that rely on an honor system for ticket purchases and the mobile inspections that appeared within the internal borders of the European Union are other examples.

Subjects may encounter repeated applications of the same means. To maximize deterrence, they may be told that there will be repetition, but not when and where. Or, when the emphasis is on apprehension, nothing is communicated. Consider checking the tickets of skiers at the top of a hill to be sure that they did not send their entry ticket down the hill to be used by someone else. To prevent drinking after a car has been started, the ignition interlock device required of those convicted of drunk driving can be programmed to require periodic tests, beyond that initially required.

Deception, in creating concern that persons and objects are other than they appear to be, is another form of uncertainty. Informers and undercover tactics are the classic deceptive examples of breaking informational borders. Hidden bugs and disguised surveillance cameras in everyday objects such as clocks, smoke detectors, towel dispensers and even Bibles are other examples. Video cameras with flashing red lights invite evasive and blocking efforts. But the visible cameras may be inoperable or not the only cameras.

Multiple Means

With the piling on of means a subject who successfully neutralizes one form may be unaware of, or unable to affect another. The use of multiple means may increase confidence in results and create greater uncertainty and resource costs for challenging subjects. It also offers a backup system should there be a failure and can provide different kinds of data –note video-cam dogs patrolling borders trained to bark at intruders.

The ratcheting up of identity and eligibility verification often follows the discovery of chicanery. To lessen switching and masking through having another's identity tokens or knowledge, several access measures may be required. Biometric measures such as facial recognition, voice and finger prints and retinal scans are ways of excluding those who may otherwise beat the system with unauthorized tokens or knowledge (e.g., of access codes) and fake identity.

Comparing an individual's voice, retinal, fingerprint, facial or DNA patterns to those in a data base, along with requiring the possession of passwords and documents offers a much higher degree of certainty, than when just the latter or a single biometric is used. Tying certification directly to the person's body lessens problems such as stolen identification and passwords. Video cameras aimed at computer users offer an additional means of identification (assuming a mask isn't worn or the camera blocked), as does typing patterns.

Procedures, Rules and Penalties

Where it is not possible to defeat neutralization via any of the prior strategies, law and policy may combat it by controlling information about tactics, prohibiting and penalizing activities and artifacts, offering rewards or legally compelling cooperation. Required standards for tools and agents may be designed to minimize successful neutralization.

Keeping information about tactics secret through classification systems and non-disclosure agreements is a natural strategic response. There are efforts to restrict and even criminalize communication about some neutralization means.

It is difficult to prevent motivated individuals from purchasing radar detectors and jammers, or to stop those under judicial supervision from the removal of an electronic monitoring device. Yet such behavior may be made less likely by applying *criminalization moves* in which neutralization leads to prison or fines and, as in the case of the anti-radar devices, confiscation. Some states have laws prohibiting the production, distribution, and use of products intended to falsify drug tests.

Some workplaces prohibit employees from encrypting their private email and phone communications. These are equivalent to anti-masking laws and signs requesting bank patrons to remove hats and dark glasses before entering. The U.S. government initially tried to ban forms of encryption that it did not control and encouraged organizations to voluntarily adopt a government provided encryption standard. It failed in this, but legislation was passed increasing penalties if encryption is used in a crime (just as penalties are greater when a weapon is used).

False reporting or failure to answer questions honestly can be grounds for legal sanctioning involving fines, imprisonment and other restrictions and/or denial of a benefit such as employment, security clearance, insurance, credit, welfare or a loan.

Cooperative moves may be engendered in the form of a more direct reward (being paid for an interview, frequent "something" awards), guaranteed amnesty or immunity). The coercive power of government may be applied as with the subpoena and testimony before a Grand Jury.

Standards for how a technology is to be manufactured and applied can involve efforts to counter neutralization. The 1994 United States' Communications Assistance for Law Enforcement Act ("CALEA") requires industries and organizations involved in telephone and internet communication to use equipment manufactured so it is readily amenable to the wire tapping of digital telecommunications switches.

Counter Counter-Neutralization and Beyond

If a tack in the shoe fails because subjects are required to take their shoes off, there are still other ways to create a pain in the posterior for agents.

Thus for the polygraph, after the addition of sensors to the subject's chair to combat sphincter contracting, the main "how to beat it" book now instead suggests tongue-biting, a move presumed to be undetectable by such means.[13]

Once restricted to police, devices for spoofing Caller-Id such that the number displayed is not the number from which the call is made are now publicly available.

In response to police use of lasers for traffic enforcement an anti-laser stealth coating can be painted on headlights which is said to reduce the targeting range for determining speed, giving the driver more time to slow down.

Sellers of anti-drug products claim continual updates (e.g., heat strips for powdered urine to pass the temperature test). In response to aerial surveillance, marijuana growers in national parks have turned to strains that are shorter and grow well in shaded areas, making them less vulnerable to discovery.

Varieties of Acceptance and Resistance

The above concepts for organizing types of resistance and response can permit the systematic analysis of variation for questions such as, "what are the correlates of the various forms of neutralization and counter-neutralization? What are the major interaction processes when neutralization and counter-neutralization are viewed sequentially?"

Yet resistance offers only part of the story. It is one end of a continuum of behavioral responses to surveillance. At the other end is acceptance. A central problem for the field should be exploring factors associated with acceptance *or* rejection.

This effort in turn needs to take account of the frequent gap between attitudes and behavior. The 12 neutralization tactics above emphasize behavioral rather than attitudinal responses. The varied relations between attitudes and behavior, between internal feelings and what is publicly presented should be eternally problematic for students of interaction and social order.

Neutralization responses are more likely to involve a "feigned" conformity and covert resistance, than direct overt resistance. More common than either of the above is acceptance (whether gladly or out of resignation, ignorance or indifference).

David Lyon (2007) captures the ubiquity and centrality of compliance:

> …we tend to take-for-granted certain kinds of surveillance….People key in their PINS, use their passes, scan their RFID entry cards, give out their Social Insurance numbers, swipe their loyalty cards, make cell-phone calls, present their passports, surf the internet, take breathalyzer tests, submit to face iris scans and walk openly past CCTV cameras in routine ways….If people did hesitate, let alone withdraw willing cooperation, everyday social life as we know it today would break down.

Concepts for organizing types of conformity are also needed. Where individuals are aware and have the potential to respond, rarely will anyone be categorically accepting or rejecting.

[13] The agent-subject polygraph interaction as a game involving rival fraudsters conning each other would indeed be humorous were its' implications not so serious. Maschke and Scalabrinin (2005) open their book with a tale of victimization and an admirable call to be honest, but then offer a rich plate of ways to deceive.

The variety of surveillance means and contexts, distinctions between attitudes and behavior, overt and covert actions and crossing personal borders by taking from or imposing upon a person can be studied for acceptance or rejection. This complexity makes sweeping generalizations unwelcome. Analyzing distinct means (e.g., video, drug testing, biometric id, location monitoring, surveys and application forms and web activity) would likely yield stronger associations than the search for general orientations. None-the-less there are likely patterns that can be studied more systematically.[14]

Robert Merton's (1957) distinction between attitudinal and behavioral conformity can be useful here. If we differentiate attitudes from behavior and accepting from resisting responses, and ignore ambivalence and fluidity, we have a fuller picture yielding four types of response for any given tool. (Table 5).

***Table 5:* Attitudinal and Behavioral Responses**

True conformists	persons who attitudinally and behaviourally accept the surveillance
Intimidated (or at least lacking resources for neutralization) conformists	persons who attitudinally reject, but behaviourally accept, the surveillance[15]
True rebels	persons who attitudinally reject the surveillance and overtly try to neutralize it
Closet rebels	persons who attitudinally reject the surveillance and covertly try to neutralize it

This table refers to subjects of surveillance. But surveillance agents too show a variety of attitudinal and behavioral responses –varying from *loyal agents* who believe in what they do and do it conscientiously, to *ritualists* who do not believe in what they area doing but need the work, to *closet rebels* who perform with indifference and even outright cooperation (if hidden) cooperation with subjects.[16] A surveillance agent as *true rebel* is rare and will likely be out of a job if discovered.

A fuller understanding of subject-agent interaction is possible when tables 4 and 5 are cross tabulated. Only a model builder in the stratosphere would bother to look at all possible combinations and then only to try to get tenure or under the influence. Yet some judicious comparison of the predominant pairings would certainly be useful. A next step is to measure the distribution and correlates of these responses across surveillance types and settings and to seek explanations for the observed patterns.

Group Resistance

Another important research question involves the connections between individual and collective responses. Understanding the conditions under which acts of individual resistance are converted to the collective organizational responses of social movements is a central question for activists, scholars and governments. The processes and social and political implications of such individual forms are relatively

[14] Marguilis, Pope and Lowen (forthcoming) and Grenville (forthcoming) offer good beginnings. The former's analysis makes clear the multifactorial nature of privacy concerns including a sense of the appropriateness of surveillance by government and the private sector and feelings about an individual's ability to control private information. They also note a generally weak link between attitudes and behavior and some major U.S.-Canadian differences.
Grenville finds that responses to surveillance (as measured by telephone survey questions) are associated with trust in the surveillance agent, knowledge and experiences with a practice and a sense of control over one's data.

[15] Beyond intimidation, this response may reflect the absence of resources for neutralization (or knowledge about them) and a non-risk taking orientation. It can also be related to deference to authority, fear of sanctioning or denial of service and exaggerated beliefs about the tool's efficacy. Politeness and the desire to avoid conflict, or be labelled a troublemaker, may also be factors.
The gap between the availability of a surveillance tool and the extent of its utilization requires a comparative measure of *surveillance slack* (Marx, 2002). So too, we can note a measure of *neutralization slack* capturing the size of the gap between the availability of resistance means and their use.

[16] Gilliom (2001), McCahill (2001) and Tunnell (2004) offer examples of the supportive agent.

unstudied systematically. That is also the case for social movements and quasi-movements challenging surveillance.[17]

How does the presence of a social movement affect individual response and vice versa? Just how individually inventive are these forms of resistance?[18] They often reflect the social currents Blumer (1957) identifies within the ethos of a broader social movement. When do they serve as a form of consciousness raising and pre-politicization in which individual resistance eventually leads to more organized political challenges? And when do they simply remain individualistic responses that inhibit such organized challenges? Under what conditions are individual responses involving subterfuge best seen as political challenges? And when are they dissipating factors that otherwise sustain the status quo?

Data on the prior (and subsequent) political behavior of surveillance resistors and their interaction with social movements and policy changes, can shed light on these issues. The point of view of those involved in the actions needs to be understood and compared to that of the outside observer. What is the impact of individual responses? In what ways are they “political”?[19] What are the connections between strategic and non-strategic responses. Are they alternatives or complementary and, when linked, what sequences are likely?

Under what conditions, are non-organizational forms of resistance effective in meeting material needs and enhancing the individual’s sense of dignity and autonomy? When do such individual actions cumulatively result in unplanned social change, apart from any formal political pressure or legal or policy changes? For example when enough people follow Nancy Reagan’s advice more broadly and just say “no” to surveillance policies, they are sometimes abandoned.[20] But under what conditions does this abandonment occur, as against resistance (if it is known about) being met with increased counter-neutralization and political efforts to gain support and compliance?

Of course the existence of resistance does not imply it will be successful and some may even be tolerated as a way of denying other realities. The silent and often non-consensual spread of technological control and personal data collection to so many areas of life means that neutralization is often not an option (or available only at very disproportionate costs). Even where possible, what does choice mean in an increasingly mechanized world? When should one be able to legitimately just say “no”?[21] Conversely in an engineered society filled with good (as well as bad) intentions, when should such discretion not be an option? Mapping the hard and soft contours and consequences of this is needed. (Marx 2006, 2008) The issue is profound and goes to the core of liberty, freedom and wellbeing in contemporary society.[22]

[17] Colin Bennett’s (2008) highly informative book on privacy activists and the incipient social movement potentials they represent is an exception.

[18] Their reiterative quality has a double meaning –referring both to the same old limited tactics and the dynamism of reciprocal innovations. What are the correlates and consequences of variation in the relative stability or change in tactics in conflict situations?

[19] In the surveillance context the limitations of such responses are considered by Martin (1998) and Monahan (2006).

[20] This was the case with Lotus Marketplace and the clipper chip. Gurak (1997) For a case study of Facebook altering its policies in response to online protest see Sanchez this issue.

[21] Twenty questions helpful in deciding the appropriateness of neutralization and surveillance policies more broadly are suggested in Marx (2007).

[22] The physical *possibility* of exercising some form of neutralizing behaviour needs to be kept distinct from situations where non-cooperation is engineered away. Within the former we can differentiate situations where refusing to provide personal data on the terms desired by surveillance agents is legitimate (as with some opting-in and out schemes) and relatively costless, from those where the refusal comes with costs that make choosing it unrealistic. These in turn contrast with situations where the possibility for resistance is illegitimate and negatively sanctioned.

References

Ball, K. (2005) Organization, Surveillance and the Body: Toward a Politics of Resistance. *Organization*, 12:1.

Bennett, C. (2008) *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

Blumer, H. (1957) Collective Behavior in *New Outline of the Principles of Sociology,* ed., A.M. Lee. New York: Barnes and Noble.

Fernandez, L. (2008) *Policing Dissent*. New Brunswick, N/J/: Rutgers University Press.

Foucault, M. (1977) *Discipline and punish: The birth of the prison*. New York: Pantheon.

Gillham, P. and Noakes, J. (2007) 'More than a March in a Circle': Transgressive Protests and the Limits of Negotiated Management. *Mobilization,* 12(4): 341-357.

Gilliom, J. (2001) *Overseers of the poor*. Chicago: University of Chicago Press.

Goffman, E. (1961) *Asylums: Essays in the social situation of mental patients and other inmates*. Garden City, NY: Anchor Books.

Grenville, A. (forthcoming) Shunning Surveillance or Welcoming the Watcher? Exploring how People Traverse the Path of Resistance. E. Zureik et al (ed.) *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons.* Queens University.

Gurak, L. (1997) *Persuasion and privacy in cyberspace: The online protests over Lotus Marketplace and the Clipper Chip*. New Haven, CT: Yale University Press.

Huey, L. (forthcoming) Subverting Surveillance Systems: Access to Information Mechanisms as Tools of Counter Surveillance in Hier, S. and Greenberg, J . *Surveillance: Power, Problems and Politics.* Vancouver: University of British Columbia Press.

Kiss, S. (forthcoming) Cell Phones and Surveillance: Mobile Technology, States and Social Movements Surveillance in Hier, S. and Greenberg, J. . *Surveillance: Power, Problems and Politics.* Vancouver: University of British Columbia Press.

Lyon, D. (2007) *Surveillance Studies*. Boston: Polity Press.

Martin, B. (1998) *Information Liberation*. London : Freedom Press

Martin, A., van Brakel, R. and Bernhard, D. (2009) Understanding resistance to digital surveillance: Towards an multi-disciplinary, multi-actor framework. *Surveillance and Society.* 6(3): 213-232.

Margulis, S., Pope, J. and Lowen, A. (forthcoming) The Harris-Westin's Index of General Concern About Privacy: An Exploratory Conceptual Replication. E. Zureik et al (ed.) *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons.* Queens University.

Marx, G.T. (2002) What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance and Society*. 1:1: 9-29. http://www.surveillance-and-society.org/articles1/whatsnew.pdf [accessed 10/03/2009]

———. (2003) A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, May 2003, vol. 59 (2). http://web.mit.edu/gtmarx/www/tack.html. [accessed 10/03/2009]

———. (2006) Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—"Hey Buddy Can You Spare a DNA?" in T. Monahan, *Surveilance and Security: Technological Politics and Power in Everyday Life.* New York: Taylor and Routledge.

———. (2007) The Engineering of Social Control: Intended and Unintended Consequences in J. Byrne (ed.) The New Technology of Crime, Law and Social Control. Momsey, N.Y.: Criminal Justice Press.

______. (2008) SWAMI, How I love Ya. Foreword to D. Wright, S. Gutwirth, M. Friedewald, E. Vildjiounaite and Punie, Y. *Safeguards in a World of Ambient Intelligence.* Springer.

McCahill, M. (2002) *The Surveillance Web*. Devon: Willan Publishing.

Merton, R. (1957) *Social Theory and Social Structure.* Glencoe, Ill.: Free Press.

Monahan, T. (2006) Counter-Surveillance as Political Intervention? *Social Semiotics* 16, 4: 515-534.

Moore, D. and Haggerty, K. (2001) Bring it on Home: Home Drug Testing and the Relocation of the War on Drugs. *Social and Legal Studies*, 10:378-395.

Murakami Wood, D. et al (2007) Surveillance in Urban Japan: A Critical Introduction *Urban Studies*, 44(3) 551-568.

Oliver, P. and Myers, D. (2003) The Coevolution of Social Movements. *Mobilization* 8(1): 1-24.

Sanchez, A. (2009) Fracas on Facebook: Resistance-Through Persistence and Resistance-Through-Distance in the Societied Network. *Surveillance and Society*. 6(3): 275-293.

Scott, J. C. (1985) *Weapons of the Weak Everyday forms of peasant resistance.* New Haven, CT: Yale University Press.

Tilly, C. (1995) *Popular Contention in Great Britain, 1758-1834*. Cambridge, MA: Harvard University Press.

Tunnell, K. (2004) *Pissing on Demand.* New York: New York University Press.

Wells, H. and Wills, D. (2009) Individualism and Identity: Resistance to Speed Cameras in the UK. *Surveillance and Society* 6(3): 259-274.