Chapter 1

An Ethics for the New (and Old) Surveillance*

Gary T. Marx

Contents

* This article draws from G.T. Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology*, University of Chicago Press, forthcoming.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

> If it doesn't look right, that's ethics.
>
> **Popular expression**

> I'm in computer science. I took this class because eventually I want to do the right thing.
>
> **MIT student**

New surveillance technologies such as the matching of computer databases, monitoring, profiling, tracking internet use, videocams, enhanced undercover activities, infrared and other searches, biometric and drug testing, and various forms of electronic location monitoring raise important social, political, and cultural questions.* In articles at www.garymarx.net, I have pursued an interest in the topic in a variety of contexts—the state, work, consumption, entertainment, and families—and identified key analytic elements such as surveillance structures and processes and means, goals, types of data, and culture.

In this work I suggest concepts to order the rich variation the topic offers across kinds of tools for collecting personal information and across various contexts regardless of whether they involve national security, work, commerce, family, or friends.

Underlying the research and interlaced with the empirical questions are moral concerns. Is a given practice good or bad, desirable or undesirable? These questions are at the core of new technologies for surveillance as a contemporary issue. However, posing questions in such a general

* For a sampling of the many discussions of the new surveillance and related themes, see Marx (1988, 2002, and 2012), Lianos (2001), Lyons (2007), and Norris and Wilson (2006). The term "new surveillance" refers to the technologically enhanced forms that extend our unaided senses ("the old surveillance") and cognitive abilities and that have expanded in power and scale so significantly in the last half-century.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

way is not helpful. The only honest answers are "yes and no," "sometimes," and "it depends." The empirical and normative task for etiquette, policy, and law is to suggest what the evaluation of surveillance does, and should, depend on.

This article stresses the contingent nature of ethical evaluation based on answers to a series of questions designed to capture the rich variation in surveillance behavior and settings. *Surveillance (or in the case of most of the chapters in this book security) is neither good nor bad, but context and comportment make it so*. Tools of course have distinctive characteristics such as the ability to see from great distances, through walls or in the dark. But whether these are right or wrong depends on the setting and goals (e.g., voyeurism, industrial espionage, legitimate law enforcement).

This chapter is organized around a series of questions for ethical evaluation that involve (1) the initial policies, procedures, and capability conditions of surveillance; (2) the characteristics of the surveillance tool; (3) the goals of surveillance; (4) the fit between means and goals; (5) data collection and analysis; (6) the consequences; (7) the rights and resources of surveillance subjects; and (8) the protection and fate of the data collected. The chapter ends with a consideration of stages of the surveillance process that the questions can be applied to.

The rich variation in surveillance across methods, goals, settings, relationships, time periods, and specific applications illustrates the importance of making distinctions—whether for purposes of social science or judgment. A situational approach to ethics is needed, rather than one emphasizing a technology or behavior in isolation from its setting or an overarching first principle to judge everything.

In studying undercover police practices for the purpose of reaching policy and ethical conclusions, I stressed the importance of rules and less formal expectations in specific contexts, rather than anything inherent in the tool (Marx 1988). This also holds for other forms of surveillance.

In writing about privacy, Nissenbaum (2010) creatively develops ideas of contextual integrity. This perspective can be applied beyond privacy to the more encompassing concept of surveillance as well.*

Simply having a technique that is morally acceptable is obviously not a sufficient condition for its use anymore than a good goal is justification for using a morally challenged or unduly risky or costly means. But even with appropriate means and ends, ethical concerns can also arise at other points such as collection, analysis, data protection, and data fate. The ethical status can vary from cases in which the means, goals, conditions of use, and consequences are wrong or even abhorrent, to those in which they are all acceptable or even desirable, to varying combinations. A more precise and richer analysis is possible when judgments are related to such distinctions.

Most contemporary disputes over domestic practices do not involve the means as such; rather they are more likely to be found in a disjuncture between the context and the means and/or the goal or to involve concern over the absence of, or failure to follow, appropriate standards for collection, analysis, and data protection. Or they involve disagreements about how a technique should be defined—is an e-mail best seen as a postcard or a first-class letter? Is a noninvasive search by a dog or a machine the same as a search by a person?

* A good summary of United States thought as of 2009 on privacy is in Waldo et al. (2007), a report of the National Academy of Sciences.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

International public opinion polls consistently show that a very large percentage of citizens are concerned about security, privacy, and surveillance issues (Zureik et al. 2010). But the elements of this are rather muddled, muddied, and inconsistent. Many persons feel a sense of discomfort in the face of indiscriminate drug testing, hidden video cameras, electronic work monitoring, airport screens, and the collection and marketing of their personal information—even as they favor security, responsible behavior, efficiency, economic growth, and credit card-aided consumption. Given the newness of the technologies, opinion here is less well defined and coherent than is the case for many more settled issues.

Persons often have trouble articulating what seems wrong with a surveillance practice beyond saying that privacy is invaded. The narrower concept of privacy is almost as confusing. What's the fuss all about? What is it about the new technology that is troubling? By what standards should we conclude that a given practice is right or wrong or at least desirable or undesirable? How should surveillance activities be judged?

Formal and abstract definitions of ethics can of course be offered based on ontological and denological principles for judging behavior. But for public policy purposes, I prefer to interrogate meanings seen in popular culture such as "if it doesn't look right that's ethics" and "you don't treat people that way." Data gathering and protection efforts imply ethical assumptions that are often unstated. In what follows, I suggest an ethical framework for thinking about the surveillance of individuals whether involving the new or traditional means (e.g., such as informing and eavesdropping). At a very general level, there are shared expectations in Western and industrial–capitalist cultures (and perhaps beyond), whose violation underlies the discomfort, or at least ambivalence, experienced in the face of many personal border crossings.

This chapter suggests some basic questions that can help identify the major factors that would lead the average person to feel that a surveillance practice is wrong or at least questionable—whether in general or in a given case. Table 1.1 lists the subjects of the questions.

I draw from examples in the literature, my interviews, and participation in various policy inquiries, court cases, and mass media accounts. The disparate violations or intrusions can be systematically located within a broader, real-world field corresponding to the surveillance occasion and context.

The analysis emphasizes the watchers rather than the watched, avoiding harm, the borders of the individual rather than the group, the short rather than the long run and domestic, and non-crisis uses rather than exceptional and emergency uses. However, many of the ideas can be applied more broadly.

The argument applies to conventional domestic settings in a democratic society for those with full adult citizenship rights. In situations of extreme crisis such as war and pandemic or when dealing with very different countries or cultures, the incompetent and dependent, or those denied juridical rights such as prisoners, a somewhat different discussion is needed and the lines in some ways will be drawn differently. The rhetoric of states of exception (Agamben 2005) or of persons of exception of course calls for extreme vigilance.

In most cases the questions are structured so that answering "yes" is likely to be supportive of a broader value and related principle. Given variation and complexity, no simple additive score is possible. Much depends. Yet other factors being equal, the more these questions can be answered in a way that affirms the underlying principle (or a condition supportive of it), the more ethical and wise the use of a tactic is likely to be.

Questions are organized according to the following categories: initial conditions; means, goals, and connections between them; data collection and analysis; consequences for subjects and others; data protection; and fate.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Table 1.1 Questions for Judging Surveillance

Formal procedure and public input in the decision to adopt
Role reversal
Restoration
Unwanted precedents
Symbolic meaning
Reversibility
Agency competence and resources
Validity
Human review
Alternative means
Appropriate goals
Goal clarity
Unitary usage
Goodness of fit between means and goals
Inaction as action
Proportionality
Criteria for subject selection
Minimization
Border crossings
Violation of assumptions
Harm in collection
Disadvantage
Unfair strategic advantage
Manipulative advantage
Restrict social participation
Damage to reputation
Betrayal of confidence and trust violation
Intrusions into solitude
Not sharing the wealth
Right of inspection

(*continued*)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Table 1.1 (continued) Questions for Judging Surveillance

Right to challenge and express a grievance
Redress and sanctions
Equal access to surveillance tools
Equal access to neutralization tools
Harm to agents
Spillover to uninvolved third parties
Periodic review
Data fate

1.1 Initial Conditions: Policies, Procedures, and Capabilities

1.1.1 Formal Procedure and Public Input in the Decision to Adopt

Does the decision to apply a potentially sensitive technique result from an established review procedure in which affected parties (whether within or beyond the organization) are consulted?* In deciding whether or not to adopt, the procedure needs to give attention to questions involving role reversal, restoration, unwanted consequences, symbolic meaning, and reversibility. These broader factors stand apart from the specifics of the tactic such as its effectiveness.

1.1.2 Role Reversal

Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects if roles were reversed? This is an aspect of the golden rule, but one restricted to an imagined shift in the organizational role played. It relates to Kant's consistency or reciprocity principle, which asks more broadly, "what if everyone used the means?"†

1.1.3 Restoration

Does the proposed technique radically break with traditional protections for personal information? Can, and should, these be reestablished through other means (whether legal or technical)? If they can't be reestablished, are new accountability procedures adopted?

Consider, for example, caller ID in potentially ending the anonymity of the caller and infrared or x-ray means that "see" through walls, clothes, and skin. Under some conditions restoration may not be desirable or possible, but then it is incumbent upon advocates to make the case for why undermining or outright destruction of the status quo is appropriate.

* For a careful examination of doing this through privacy impact assessments, see Wright and de Hert (2012). Many other impacts can be noted in equivalent assessments as well.

† Other strands of a broader equality question: "Are the tools equally available to all in situations where reciprocity is appropriate?" or "Is the tool applied equally to all subjects?"

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

1.1.4 Unwanted Precedents

Is the tactic likely to create precedents that will lead to its application in undesirable ways? What unwanted consequences might the tactic have for subjects, agents, third parties, and society more broadly? How might traditional liberties and basic democratic values be affected? Will a tactic lead opponents to turn to the same tactic?

1.1.5 Symbolic Meaning

Do the tool and the way it is applied communicate a view of citizens with rights appropriate for a democratic society? Or is the individual subject viewed as an object without rights who must be subservient to the interests and greater power of an organization entitled to indiscriminately apply invasive and even degrading techniques? The standards for assessing symbolic communication are more subjective than for many of the other questions.

1.1.6 Reversibility

If subsequent experience were to suggest that the tactic is undesirable, how easily can it be ended in the face of large capital expenditures and vested interests backing the status quo?

1.1.7 Agency Competence and Resources

Does the organization have the resources, skills, and motivation to appropriately and effectively apply, interpret, and use the tactic? Does it engage in critical self-reflection in the use of sensitive techniques? For example, in the case of undercover police practices that can be effective, the discussion is not about the worth of the tactic but whether the risks it brings can be adequately managed given the agency's policies and resources. Similarly some of the criticism of the United States' Transportation Security Administration is not about its technology but about whether the agency's personnel have adequate training and competence to apply it.

1.2 Means

1.2.1 Validity

Is the tactic valid with respect to both its potential for accurate measurement and a given application?—a valid tactic can be wrongly applied or in error or the tactic can be insufficiently reliable. How much agreement is there among specialists about the merits of a tactic? Validity is in part a socially constructed concept. As the philosopher Alfred Whitehead observed, "Everyway of seeing is also a way of not seeing." Awareness of this brings the question, "Say's who?" How are claims of validity defined—what degree of certainty is deemed necessary for strong conclusions and actions based on the results? How are the lines drawn between "acceptable" and "unacceptable" levels of proof?

1.2.2 Human Review

Are there means to verify results and periodic checking on the tool itself? Is there human review of machine-generated results—both basic data and (if present) automated recommendations for

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

action? In many settings, human checking of automated findings and recommendations is vital given the acontextual nature of the data and risks of hardware and software failure.* Generally, individuals as interpreters of human situations are far more sensitive to nuance than are computers, even if they are more expensive and corruptible.

1.2.3 Alternative Means

Is this the best available means? How does it compare to other tools with respect to ethics, ease of application, validity, costs, risks, and measuring outcomes? Is there a tilt toward counting (in both senses) what can most easily and inexpensively be quantitatively measured, rather than toward what is more directly linked to the goal?

1.3 Goals

1.3.1 Appropriate versus Inappropriate Goals

Are the goals of the data collection legitimate and consistent with the information expectations of the setting? Is there a strong rational for pursuing the surveillance goal within the environment in question?

Relatively noncontroversial, positive goals such as health and protection are easier to identify than their opposites. The latter, by their very nature, are likely to be hidden under the camouflage of acceptable goals.

A data collection goal acceptable in one context may be unacceptable in another. Consider the following contrasting cases:

- Drug testing school bus drivers versus junior high school students who wish to play in the school band (as has happened in the United States)
- Electronic eavesdropping carried out by a national security agency subject to strong policy and law versus that done by a domestic political party against its opponents (as was the case with President Richard Nixon in the Watergate scandal)
- A doctor asking patients about sexually transmitted disease, birth control, and abortion history in a clinical setting versus asking this of all female employees (as one large U.S. airline did) without indicating why the information was needed

But even when the goal is right for the setting, if results of the surveillance spill over into other settings, controversy is likely. For example, is it appropriate to use a pulmonary lung test to measure whether employees are in conformity with a company's nonsmoking policy? Employees are told that this is a necessary health and cost-saving measure—good for the company, the other workers, and the employee. But some employees see this as wrong because it seeks to control their behavior away from the job—behavior they have a legal right to engage in.

* For example, in an early Massachusetts computer matching case, a list of those on welfare was compared to a list of those with more than $5000 in the bank (the cutoff point for being on welfare). Those on both lists had their welfare payments automatically terminated with no further checking (Marx and Reichman 1984).

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

1.3.2 Clarity in Goals

Is the goal(s) clearly stated, justified, and prioritized (if more than one)? Where secrecy is appropriate and the goals are not publicized, have they been clearly defined within the organization? Is there broad consensus on the goals?

1.3.3 Unitary Usage

Are data used for the purpose for which they were collected consistent with the subject's understanding (and where appropriate agreement)? Do the data remain with the initial agent/owner or migrate? If the latter, is this because of a failure to maintain confidentiality and security of the data? In the United States to a much greater extent than in Europe, second, third, fourth, and more users and uses are common. Combining data from different sources gathered for different reasons through computer matching, profiling, and mining can yield information in which the sum exceeds the individual elements. As such it constitutes a new kind of involuntary search not envisioned by traditional human rights protections against unreasonable searches and seizures and requires careful debate.

1.4 Connections between Means and Goals

1.4.1 Goodness of Fit between the Means and the Goal

Is there a clear link between the information sought and the goal to be achieved? How well a test measures what it claims to—truth telling, drug and alcohol use, miles driven, or location—can be differentiated from second-order inferences made about goals only indirectly related to the actual results of the measurement such as risk predictions. A measure can be valid in its immediate empirical results without being effective with respect to a goal.*

As we move from the direct results of a measure that is immediately meaningful given the goal (e.g., heat or location data from a sensor to more removed goals based on probabilistic inferences about future behavior) as with profiles, usefulness of the data often lessens. A profile such as one used to predict airline highjacking (young males buying one-way tickets paid for with cash) involves very accurate data but a very weak correlation to subsequent incidents.

Urine drug tests, when properly done and backed by a second confirming test, show high validity. Yet some research suggests that drug tests may not be associated with the employment performance behaviors they are presumed to predict. In that regard, drug tests based on manual dexterity for drivers of trucks, buses, and taxis may offer a better fit than the more inferential urine drug tests.

1.4.2 Inaction as Action

Where the only available tool is costly and/or risky or weakly related to the goal because what is of interest is difficult to detect or statistically very unlikely to occur, has consideration been given

* Valid that is in what it measures. It can also be effective but not valid via the mechanisms claimed. Note the polygraph that "works" when individuals confess in the belief that the machine can tell if they are lying.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

to taking no action or to redefining the goal? For example, the arguments for decriminalizing marijuana point to the failure of enforcement efforts and the many unwanted consequences.

1.4.3 Proportionality

Do means and ends stand in appropriate balance? This requires attention to the potential problems and gains from the means and the importance of the goal. A sledge hammer should not be used to crack open a nut, nor a sprinkling can to put out a house fire. Hanging them all will likely get the guilty, but unduly stringent restrictions will mean subjects deserving of scrutiny (and worse) may escape.

1.5 Data Collection and Analysis

1.5.1 Criteria for Subject Selection

Are universalistic standards applied? Where there are no grounds for treating persons differently, are all subject to surveillance or do all have an equal chance of being surveilled, even if few are actually chosen?* For example, contrast categorical scrutiny within a group, as with checking names of all flyers against no fly lists, against selecting a few subjects for an intensive customs border search based on a table of random numbers. When there are no easily identifiable correlates of what is looked for, preliminary superficial screening of everyone may be used to identify cases for a more intensive gander.

1.5.2 Minimization

Is there an effort to minimize the invasiveness of the tactic and the extent of personal and personally identifiable information collected? This cuts across other questions such as alternative means, goals, specificity in subject selection and data collection, and the related ability to control spillover. Other factors being equal, a less invasive tactic is preferable, only personal information directly related to the goal should be collected and then no more than is required.

1.5.3 Border Crossings

Does the technique cross a potentially perilous personal boundary without notice or permission (whether involving coercion or deception or a bodily, relational, spatial, or symbolic border)? If consent is given, is it genuine?

1.5.4 Violation of Assumptions

Does the technique violate assumptions that are made about the conditions under which personal information will be collected? This can involve standard, often tacit, cultural expectations such as that persons are who they claim to be, that conversations will not be secretly reported, that confidences will be respected, or that there will be no secret government blacklists. It can also involve

* The consistency principle here, which asks whether the tactic is applied to everyone, is different from asking what if everyone applied it.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

failing to honor explicit policies or promises such as that data will be destroyed or not shared or used only for purposes consistent with stated intentions.*

1.5.5 Harm in Collection

Does the act of data collection involve physical or psychological harm? Some interrogation tactics (e.g., as against passive data collection) are based on the creation of fear and threats to inflict harm as a bargaining tool. Torture is the obvious example. But a data collection, particularly in face-to-face settings, need not involve the threat of violence to be stressful or ethically questionable.

Interviews, psychological tests, drug tests, and searches can be done to minimize or maximize discomfort. Being questioned about sensitive subjects and having personal data gathered may necessarily involve some feelings of embarrassment, shame, discomfort, powerlessness, and recalling or reexperiencing painful memories. The agent's manner and the conditions of data collection however can exacerbate these. The agent may go farther than is required or than has been publicly announced (and perhaps agreed to by the subject). Consider intentionally inflicting pain in drawing blood (e.g., in the mandatory AIDS tests required of those in prison and the military) or added stress in the application of the polygraph (e.g., by making the cuff tighter than necessary).

1.6 Consequences

1.6.1 Disadvantage

Are the results used to cause unwarranted disadvantage or harm to the subject, the agent, and the third parties? There is of course much room for debate over this and whether it should be defined in objective or subjective terms and whether the intentions of the agent should be considered apart from measurable consequences.

Some common forms include the following:

1. *Unfair strategic advantage* in discovering information the subject wishes to withhold in situations where there is a legitimate conflict of interest. Consider a bugged car sales waiting room, which permits the seller to learn a customer's concerns and maximum payment or corporate espionage.
2. *Manipulative advantage* in persuading or influencing a subject whether involving consumption or politics. At the extreme is blackmail and intimidation. But consider the more benign form of a candy company mailing a special discount offer to a list of diet workshop participants it had purchased.
3. *Restrict social participation* or otherwise unfairly treat persons based on information that is invalid, irrelevant, acontextual, or discriminatory. Many examples are in health insurance, banking, housing, employment, and even chances for consumption. Oscar Gandy (1993) has noted how market research on consumption behavior can work to the disadvantage of the least privileged.

* This is particularly likely to be an issue for political databases. Consider the case of Greece (Samatras 2004), for example, where government claims to have destroyed prohibited political databases were reputed to simply have been transferred to private holders. The failure to create documents—for example, not having audiovisual equipment on or failing to record and save when the rules require—presents an opposite problem.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

4. *Damage to reputation* as a result of unwarranted publication or release of personal information that causes embarrassment, shame, humiliation, or otherwise puts a person in a negative light.*
5. *Betrayal of confidence and trust violation* may occur (even if the information is neutral or positive for the subject). This is distinct from hurtful content, procedural violations, and exaggerated claims. Trust is a central element in spontaneity, sociability, and communality. Its absence makes cooperative group action difficult. A belief that one is continually monitored can inhibit innovation and experimentation and eliminate risk taking.
6. *Intrusions into solitude* as a result of the collection and use of surveillance data may deny the individual the ability to control the access others have to them. The act of data collection may perturb the individual's sense of personal space and expectation of being left alone. The indiscriminate use of discriminate results may result in targeted marketing via uninvited use of the subject's communication resources (fax, phone, computer) and time.
7. *Not sharing the wealth*—is the additional benefit or profit a company or a data warehouse gains from selling an individual's personal information shared with the subject? Has the individual given permission for the reuse and sale of the data?

1.7 Agents and Third Parties

1.7.1 Harm to Agents

Does the tactic avoid harm to the agent? Are there undesirable impacts on the values and personality of the surveillance agent? Can the risks be reduced or mediated? Consider super electronic sleuth Harry Caul in the film "The Conversation." Over the course of his professional career, Caul becomes paranoid, devoid of personal identity, and desensitized to the ethical aspects of his work. Undercover police agents face a variety of risks from attack to crime temptations to psychic and family costs. There is some evidence that police who use radar guns in traffic enforcement have higher rates of testicular cancer.

1.7.2 Spillover to Uninvolved Third Parties

Can the tactic be restricted just to subjects? Can undesirable effects on others be avoided? How focused and contained is the tactic? Audio- and videotaping may record the behavior of subjects as well as that of their family and friends; DNA may offer information on family members whose DNA was not collected.

1.8 Data Protection and Fate

1.8.1 Periodic Review

Is the system regularly reviewed for effectiveness, efficiency, fairness, and operation according to policies (or the need for new or revised policies)? Are there audit trails and inspections?

* The embarrassment caused by the falsely accused is a rarely considered form—for example, an invalid result such as having an alarm go off by mistake as one walks through a detection device in a store or library or the rejection of a valid credit card.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

1.8.2 Data Fate

Are there rules regarding the retention, conditions for sharing, and destruction of the data, and are these honored?

1.9 Rights and Resources of Subjects

Right of inspection: Are subjects aware of the findings and how they were created? Fundamental aspects of procedural justice involve the right to know and challenge the evidence in the face of the haze of bureaucracy experienced by Franz Kafka. In the case of government, the right to have access to one's file is related to a broader principle that, absent special conditions, there should be no secret personal databases in a democratic society.

Right to challenge and express a grievance: Are there procedures for challenging the results and for entering alternative data or interpretations into the record?

Redress and sanctions: If the individual has been wronged, are there means of discovery and redress and, if appropriate, for the correction or destruction of the record? Are there means for minimizing or preventing such problems? Are there audits and sanctions to encourage responsible surveillant and fair and just outcomes?

Unlike Europe and Canada where there are official data commissioners who may actively seek out compliance, in the United States, it is generally up to individuals to bring complaints forward. But in order for that to happen, they must first be aware that there is a problem and that there are standards.* Internal agents such as inspector generals, auditors, and public interest watchdog groups are other means of identifying problems. The development of privacy officers within organizations is a recent tool. How independent and effective they can be given their host is a challenging organizational question.

Equal access to surveillance tools: In settings of reciprocal (or potentially reciprocal) surveillance, are the means widely available or disproportionately available (or restricted) to the more privileged, powerful, or technologically sophisticated? Contrast the ability to use satellite imagery with the cell-phone camera. Must doctors reveal personal information (e.g., investigations by professional boards) to patients, just as patients may have to agree to a search of a database to see if they have ever sued a doctor?

Equal access to neutralization tools: In settings where neutralization is legitimate (whether because the rules permit it or because unwarranted agent behavior may be seen to justify it), are the means widely available or limited to the most privileged, powerful, or technologically sophisticated? Some means of maintaining control over personal information such as providing a false name and address when the request is irrelevant (as when paying with cash at a store) or free anonymous e-mail forwarding services are available to anyone. In other cases, protecting information may require technical skills or come with a price, as with the purchase of a shredder, an unlisted phone number, or otherwise purchasing a higher level of privacy.

* This is the discovery of dirty data issue. Among common means of discovery are accidents, tests, informers, and deduction (Marx 1984).

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

1.10 Questions about Questions

As suggested, the more the principles implied in these questions are honored, the more ethical the situation is likely to be, other factors being equal—which of course they rarely are given, among many other concerns, the importance of prioritizing and weighing values. The questions require several kinds of evaluation.

Are there procedures and policies covering the basic areas? Questions can then be asked about substance—are they good policies? Are the policies followed in practice? Does the organization (or others) regularly check on itself through audits and inspections? Is the subject likely to be aware when a policy fails?

Inquiring if the policies are followed can be looked at across all, or a sample of cases, as well as in any given case. For example, the validity and consequences of a specific type of drug testing as a class can be considered. But questions can also be asked about the application in a given case.

Distinctions are also needed between rejecting, limiting, or revising a tactic such as the polygraph because of questions about its efficacy, as against rejecting a particular flawed application of an otherwise acceptable tactic.

When failings are identified, it is vital to know if they are idiosyncratic and seemingly random or are systemic. Is it the apple or the barrel? How often do individual problems have to appear before it is concluded that the problem is in the system rather than an unfortunate, but tolerable, occurrence? If it is the former, can it be fixed?

If answers to the earlier questions are supportive of adopting a new technique, it is then necessary to ask about the presence of policies and resources for managing it. Are there policies and procedures for guaranteeing the integrity, fairness, and effectiveness of the system? The ability and will to develop such policies should be a necessary condition for adoption of an otherwise acceptable technique. Policies will cover who agents and subjects are; their rights and responsibilities; how and when data are to be collected, merged, altered, analyzed, interpreted, evaluated, used, communicated, protected, updated, or purged; and internal and external oversight.

1.10.1 Surveillance Stages

An additional analytic perspective is provided by identifying stages of activity. Table 1.2 lists seven kinds of activity called *surveillance strips* that follow each other in logical order. The strips are temporally, conceptually, empirically, and often spatially distinct.

Table 1.2 Seven Surveillance Strips

1	Tool selection
2	Subject selection
3	Data collection
4	Data processing/analysis (raw data) numerical/narrative
5	Data interpretation
6	Uses/action—primary, secondary uses/users and beyond
7	Data fate (made public, restricted, sealed, destroyed)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Over time, the distinct action fragments of these stages combine into stories about personal data and illustrate the emergent character of surveillance and privacy as multifaceted abstractions made up of many smaller actions. These are not unlike the frames in comic books (although not intended to be entertaining and the patterns are more like the fluid, jumpy sequences of cyberspace explorations than the rigid frame ordering of the comic book).

When viewed sequentially and in their totality, these elements constitute *surveillance occasions*. A surveillance occasion begins when an agent is charged with the task of gathering information. Following that, the seven phases in Table 1.2 can be considered.* Studying the behavioral sequences of tool selection, subject selection, data collection, data processing, interpretation, resulting action (or inaction), and fate of the data offers a way to order the basic behaviors occurring within the family of direct surveillance actions.†

The questions in Table 1.1 may cut across various stages of the surveillance process or be restricted just to one. Awareness of the sequential stages of data generation and use can help anticipate and locate problems. The stages are the direct pressure points where most problems will be found and questions can be asked about ethics for each.

The kind of problem may differ by stage—thus violations of consent are likely at data collection, of fairness and validity at processing and interpretation, of discrimination at use, and of confidentiality at data fate.

It would be useful to have a checklist of problems that can occur and (when possible) of ways of avoiding them or ameliorating them when they can't be prevented. As implied by the questions earlier, the list would include various kinds of physical, psychological, and social harm and unfairness in application and use; minimizing invalid or unreliable results; and not crossing a personal boundary without notice or permission (whether involving coercion or deception or a body, relational, spatial, or symbolic border). Other problems to be avoided involve violating trust and assumptions that are made about how personal information will be treated (e.g., no secret recordings, respect for confidentiality, promises for anonymity, for the compartmentalization of kinds of data, and for their protection or destruction).

Awareness of the stages can direct research on the correlates and location of particular kinds of problems. This can contribute to assessing the seriousness and likelihood that a risk will occur and the costs of prevention (whether by not using, regulating, or amelioration after the fact).

The likelihood of prevention is also greatly affected by the stage. Just saying "no" to a data collection request (if honored) is the ultimate prevention. But as the process moves from collection to the final fate, controls become more challenging. In the initial stages, the relevant actors and locations for accountability are known—but over time, if the information spreads out in wider circles and is combined with other data, as often happens, control weakens. The form of the data matters as well—type of format, encryption, self-destroying, and identity masking—in a single highly secure file or a more open system.

---

* Decisions about *who* is responsible for doing the surveillance and the design of the technology could be treated as the initial strips as well. However, attention here is on the next stage directly associated with doing the surveillance.

† This is said mindful of the fact that it is always possible to make ever greater differentiations within the categories identified and to push the causal chain back farther. For example, with respect to the data collection phase, contrasts can be made based on the tool, the sense involved, the kind of activity, or the goal. Yet I think Table 1.2 captures the major natural breaks in activity once a problem in need of surveillance is identified.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

1.11 Conclusion: Complexity Yes, Abstention No

In the best of all possible planets, for the philosopher an ethical theory needs to be grounded in a formal normative argument that offers justifications for its principles, indicates their logical implications, and leads to clear conclusions. Such an argument would anticipate and respond to likely objections and would be consistent across types of justification (e.g., it would not mix arguments based on categorical first principles with those based on empirical consequences as is done here).

Like a kaleidoscope with a unifying light source, an integrated ethical theory should illuminate and link the varied shapes of surveillance.* It would be nice if the world had been created such that a simple deductive Rosetta stone for judging surveillance was possible. But given the world in which we live, such an effort would need to be so general and banal as to be of modest interest or use ("do good, avoid harm").

The alternative offered here—an inductive approach that asks about the ethics of heterogeneous settings and behavior—also has limitations. A comprehensive consideration of the myriad factors that can go wrong or right with surveillance may overwhelm the observer. Casting such a wide, yet thinly meshed, net brings the risk of being unwieldy and unrealistic, let alone unread.

This can easily lead to the search for quick solutions ignoring complexity and moral conflicts. There is the danger of denying the requirements of the "dirty harry problem" in which there are costs associated with whatever action is taken (Klockars 1980). There is also the risk of accepting the fallacy of quantification—falling back on automatic bureaucratic decision making based on ethics by the numbers (e.g., simply counting up the "yes" and "no" answers to the questions in Table 1.1 and declaring the majority wins).

I have sought an intermediate position—casting a net broad enough to capture the major sources of variation and filtering these through some basic values. This chapter's emphasis on surveillance agents reflects concern over the abuses that can be associated with the tilted nature of private sector, organizational and authority playing fields, and unequal access to surveillance resources. Yet the demonology and glorification involved in viewing data gatherers as invariably up to no good and surveillance subjects as helpless victims whose rights are always trampled need to be avoided.

We all play multiple roles and rotate between being agents and subjects. Organizations and those in positions of authority are prone to give greater emphasis to their rights to gather and use personal information than to their duties or to the rights of subjects. Subjects generally show greater interest in protecting their own information than in the informational rights of others and are relatively unaware, or uninterested, in the information of organizations.

Under appropriate conditions, agents have a right and even an obligation to surveil, but they also have a duty to do it responsibly and accountably. Reciprocally, those subject to legitimate surveillance have obligations as well (e.g., not to distort the findings or threaten agents), even as they also have rights not to be subjected to some forms of surveillance.

In spite of all the factors (whether contextual or inherent in values) that work against broad generalizations about the ethics of surveillance, some moral threads that swirl within and between the questions can be noted.

* Thus, it would need to take account of the behavior of individuals, organizations, states, and the international order as these involve crossing borders to impose upon and to take from subjects; the rights and obligations of various parties; the ethical meanings of doing good and avoiding harm; and various levels of analysis such as kinds of institutions and roles, the cross-cultural, and the short and long run.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Some values are desirable as ends in themselves (e.g., honesty, fairness). But values may also be a means to some other ends (e.g., democracy as a support for legitimacy, privacy as a support for intimacy or political organization, transparency as a support for accountability).

In democratic societies operating under the rule of law, a cluster of value justifications underlie the questions raised. The most overarching and important is the Kantian idea of respect for the dignity of the person and respect for the social and procedural conditions that foster a civil society.

References

Agamben, G. 2005. *States of Exception*. Chicago, IL: University of Chicago Press.

Gandy, O. 1993. *The Panoptic Sort*. Boulder, CO: Westview Press.

Klockars, C. 1980. The dirty harry problem. *The Annals* 452: 33–47.

Lianos, M. 2001. *Le Nouveau Controle*. Paris, France: L'Hamilton.

Lyons, D. 2007. *Surveillance Studies: An Overview*. Cambridge, U.K.: Polity Press.

Marx, G.T. 1984. Notes on the discovery, collection, and assessment of hidden and dirty data. In *Studies in the Sociology of Social Problems*, Eds. J. Schneider and J. Kitsuse. pp. 78–114. Norwood, NJ: Ablex.

Marx, G.T. 1988. *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.

Marx, G.T. 2002. What's new about the 'new surveillance'?: Classifying for change and continuity. *Surveillance and Society* 1(1): 9–23.

Marx, G.T. 2012. 'your papers please' personal and professional encounters with surveillance. In *International Handbook of Surveillance Studies*, Eds. D. Lyon, K. Ball, and K. Haggerty.

Marx, G.T. and Reichman, N. 1984. Routinizing the discovery of secrets: Computers as informants. *American Behavioral Scientist* 27(4): 423–452.

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.

Norris, C. and Wilson, D. 2006. *Surveillance, Crime and Social Control*. Hampshire, U.K.: Ashgate.

Samatras, M. 2004. *Surveillance in Greece*. Pellas, NY: Pella Press.

Waldo, J. et al. 2007. *Engaging Privacy and Information Technology in a Digital Age: Issues and Insights*. Washington, DC: National Academies Press.

Wright, D. and de Hert, P. 2012. *Privacy Impact Assessments Engaging Stakeholders in Privacy Protection*. Dordrecht, the Netherland: Springer.

Zureik, E. et al. (Ed.). 2010. *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*. Montreal, Quebec, Canada: McGill-Queen's University Press.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security

Balancing Technology and Social Issues

Edited by
Francesco Flammini • Roberto Setola • Giorgio Franceschetti

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20130401

International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Library of Congress Cataloging-in-Publication Data

Effective surveillance for homeland security : balancing technology and social issues / editors, Francesco Flammini, Roberto Setola, Giorgio Franceschetti.
pages cm. -- (Multimedia computing, communication and intelligence)
Includes bibliographical references and index.
ISBN 978-1-4398-8324-2 (hardcover : alk. paper)
1. Electronic surveillance. 2. Video surveillance. 3. Privacy, Right of. 4. National security. I. Flammini, Francesco. II. Setola, Roberto. III. Franceschetti, Giorgio.

TK7882.E2E42 2013
363.325'1630973--dc23 2013008817

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To Liana, Lucia, and Giuliana:

amare et sapere vix deo conceditur.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Contents

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

PART II PHYSICAL AND CYBER SURVEILLANCE

PART III TECHNOLOGIES FOR HOMELAND SECURITY

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Foreword

The September 11, 2001, terrorist attacks shocked the entire world—the scale of devastation inflicted by this horrific attack still evokes a spine-chilling reaction today! More than a decade later, the events on that day still impact us in various ways and at different levels—from our increased awareness of the threat in our day-to-day lives to the augmented security measures, known and unknown, that are in place to protect us. The recognition that the threat of terrorism can range from the macro to the micro scale has changed how homeland security forces in different countries think about interdiction and the way in which governments, business, and insurance industry manage potential loss as a result of any terrorist activity.

The threat of terrorism persists with us, despite the formation of an alliance of the Western nations to eradicate it completely, and it is an unfortunate reality that this threat will continue in some form for many years to come. The security and counterterrorism intelligence alliance of the Western countries has played a crucial role in controlling the frequency of the attacks and minimizing their impact in the United States and Europe. Unfortunately, in other countries, especially those in the Asian and African continents, terrorism still rages with less interdiction success, and more than 25,000 people worldwide are estimated to have died in militant Islamic terrorist attacks since the catastrophic attack on 9/11.

The sheer scale and magnitude of the 9/11 attacks, executed by a network of terrorists intent on triggering simultaneous events causing mass destruction and loss of human lives, stunned the entire world and moved the threat of terrorism to the top of security priorities in many countries around the globe. In addition to causing significant loss of life and physical destruction, the attacks also resulted in one of the most costly insurance events in the history of the world.

In a presentation to the South West Regional Chapter of the INMM (Institute of Nuclear Materials Management) in 2002, Sig Hecker of Los Alamos National Laboratory characterized the tragedy of 9/11 as the third seminal event in the history of mankind—the first being the dropping of atomic bombs on Japan, and the second the fall of the Soviet Union. Hecker believed that the world's response to 9/11 would be our "third chance" to create a promising future for mankind. However, he also pointed out that if the right actions are not properly taken, the event might plunge the world into a detrimental future. He hoped that using various tools of scenario planning, a future world could be created that would provide the environment for strategic discussion among global leaders, so that even more significant events than 9/11 could be prevented or mitigated.

Dr. Hecker was not wrong in his observation. In the aftermath of the 9/11 attack, infrastructure security has become the top priority of the governments of all countries and many commercial organizations. The most critical infrastructures include banking and finance, telecommunications,

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

energy (gas and electricity), water distribution, transportation, emergency services, and essential government services. Any damage or destruction of these critical infrastructures would have a crippling effect on the defense and economic security. Moreover, these infrastructures are so interconnected that the failure of one will adversely affect the operations of the others. Hence, safety and security of these infrastructures have become extremely critical after the deadly attack on 9/11. As rightly predicted by Hecker, meeting the test of terrorism today requires a proactive approach to the technological innovation—consolidating on the present and betting on the future: formulating clear requirements, prioritizing the needs, establishing cooperative means to foster the development of technologies, and building the human and financial capital program necessary to transition and sustain them as effective antiterrorism tools.

It is not very difficult to understand that technology is not the only answer to address the devilish specter of transnational terrorism. However, it is a hard truth that the technological answers we have today are inadequate to deal with the scope and potential severity of the threat that pervade us. Instead of merely adapting technologies to keep pace with the evolving dangers and changing tactics of terrorism, what is needed is to develop more powerful and overmatching security systems to get ahead of the terrorists. Adoption of a proactive and well-thought security strategy can only ensure that the public is protected, their liberties are safeguarded, and commerce, business, and critical emergency operations can continue unhindered. Developing technologies that leap ahead of those in the hand of the terrorists requires vision and strategy, and a good strategy requires hard choices. Adopting some of the current technologies is also important for this purpose. Some of the existing information-searching and analytical approaches that can be adopted to counterterrorism domain are (i) the use of the existing general-purpose and meta-search engines, (ii) terrorism research centers' portal, (iii) information analysis techniques, (iv) social network analysis, and (v) chatterbot techniques. However, the research on certain technologies can lead to the development of novel techniques to counterterrorism such as (i) biometrics, (ii) development of nonlethal weapons, (iii) data mining and link analysis technologies, (iv) nanotechnologies, (v) image and video processing, (vi) intrusion detection and access control, and (vii) directed-energy weapons.

However, mere adoption of current technologies is not enough. We need innovations for developing new technologies to counterterrorism. For example, in addition to traditional biometric techniques such as iris recognition, hand geometry analysis, fingerprint recognition, face recognition, voice recognition, and DNA matching, some novel biometric techniques may be used, such as odor sensing, blood pulse measurements, skin pattern recognition, nail bed identification, gait recognition, and ear shape recognition.

Development of nonlethal weapons can be a new addition to the armory of counterterrorism mechanisms. These weapons should be explicitly designed and deployed to incapacitate or destroy terrorists or dangerous materials while keeping their impact on the facilities and the environment at a minimum. Research conducted by the US military has shown that there are four promising areas in the development of nonlethal weapons: (i) calmatives for controlling crowds and clearing facilities, (ii) directed-energy systems that work on high-power microwave for stopping potentially dangerous vehicles or vessels, (iii) novel and rapidly deployable marine barrier systems, and (iv) adaptation of unmanned or remotely controlled platforms and other sensors for application of nonlethal weapons.

Design of advanced data mining algorithm for carrying out complex analytics on the humongous volume of historical and current online data to identify patterns and anomalies is an important direction of research for counterterrorism mechanism development. Link analysis is another analytical approach that can be gainfully exploited in developing counterterrorism

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

systems. While data mining attempts to identify anomalies in large volume of information, the objective of link analysis is to search for commonalities among the datasets. In identifying terrorist activities, link analysis is used to analyze the data surrounding the suspect relationships to determine how they are connected—what links them together. The research on data mining and link analysis needs to be augmented to handle unstructured and disparate data consisting of a mix of text, image, video, and sensor information. In addition, new algorithms need to incorporate knowledge of human experts into their derivation patterns.

Development of nanoscale sensors is another emerging area of counterterrorism applications. Nanodevices can be used to design fast, cheap, and accurate sensors and actuators that can be used for a wide range of forensic activities.

Active defenses such as directed-energy weapons could provide protection to the critical infrastructures. In contrast to conventional weapons that rely on kinetic or chemical energy of a projectile, directed-energy weapons can hit a target with subatomic particles that can travel at the speed of electromagnetic waves. These weapons generate very high power beams and typically use a single optical system for tracking a target and for focusing the beams on the target in order to destroy it.

There are daunting barriers to the creation of an arsenal of counterterrorism technologies that are efficient, yet cost-effective, and that can overpower the threat of terrorism in the twenty-first century. However, it is mandatory to create a vision of these future technologies, implement initiatives that broaden the market of these technologies and make them more dependable, and develop policies that would help in overcoming the barriers to innovation and research. In this way, these technologies can be harnessed to the future needs of law enforcement and countering terrorism.

The objective of this book entitled *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*, edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti, is to discuss the various technological aspects related to homeland security solutions. It also focuses on privacy and other related social issues, which are of conflicting interests with the surveillance operations necessary for working of homeland security solutions.

The book is especially useful for engineers and researchers working in the area of homeland security solution design and development, people working in the law enforcing agencies, operators of critical infrastructures, and researchers and people who are in the decision-making position for establishing security policies and infrastructures for safety and security of citizens and critical infrastructures. It is also useful for graduate students and faculty members working in graduate schools and universities.

Jaydip Sen
Senior Scientist
Tata Consultancy Services Ltd.
Kolkata, India

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Preface

It is a common feeling for people living in developed countries that their privacy is being increasingly threatened by surveillance and tracking technologies. The fact that surveillance is essential to reduce criminal acts is only partially supported by evidence, and that raises big questions about the effectiveness of technologies and of how they are managed.

This book, *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*, addresses two aspects of surveillance: (i) advances in technology developments and (ii) their social impact in terms of privacy and human-related factors.

Quite obviously, when monitoring public areas, Internet usage, or working personnel, increasing surveillance means decreasing privacy. Therefore, the challenge is twofold:

1. To provide evidence that technology is actually effective for deterrence, prevention, and timely reaction
2. To make technology as much as possible noninvasive and respectful of privacy, ergonomics, and wellness

The issue becomes even more delicate when surveillance aims at addressing the complex and multifaceted problem of homeland security.

Most developed countries addressed the issue of privacy by appropriate laws and norms. As an example, the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) regulates the process of acquisition, management, and storage of personal data within the European Union (EU), being an important component of EU privacy and human rights law. Most of us are aware of the impact of such laws on our everyday life, since they define many rules on video surveillance installations (e.g., mandatory signs and constraints on watched areas) and on the management of personal data (e.g., when registering on websites).

At the same time, as legislation defines appropriate regulations about surveillance, tracking technologies have advanced in such a way as to be able to control the behavior of millions of people 24 h a day: it suffices to think of high-resolution satellite imaging, people scanning, RFID tagging, intelligent multimedia (audio–video) analytics, web surfing monitoring, etc.

With this background in mind, it is easy to imagine the importance of a book addressing the often neglected aspects of advanced surveillance, filling a gap existing in the related literature between technology developments and the delicate issues related to their social impact.

The book consists of 21 chapters written by experts in different aspects of homeland security. These chapters deal with three broad areas: (i) surveillance technologies; (ii) legislative and social

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

aspects of homeland security operations; and (iii) advanced issues on surveillance operations, such as advanced analytics and multimodal surveillance.

Book Structure

According to a scheme that is unusual in technical books on security and surveillance, Part I—Surveillance and Society is not dedicated to technological aspects, focusing instead on the societal dimension of surveillance. This choice stresses the importance of societal acceptability as a precondition to any surveillance system.

Starting from that general picture, Part II—Physical and Cyber Surveillance focuses on advanced technologies for surveillance. Most of those developing technologies are part of a framework whose aim is to move from a simple collection and storage of information toward proactive systems, able to fuse several information sources in order to detect relevant events in their early incipient phase. Such a trend leads to security information management systems that are increasingly smart.

Finally, some relevant applications of surveillance systems used in the framework of homeland security are collected in Part III—Technologies for Homeland Security in order to show via real-world case studies how innovative technologies can be used to effectively improve the security of sensitive areas without violating the rights of involved people.

In what follows, a more detailed description of the parts of the book, providing insights on the content of the chapters is provided.

Part I: Surveillance and Society

In Chapter 1, "An Ethics for the New (and Old) Surveillance," Marx discusses how various types of surveillance can be analyzed. More specifically, the author stresses on the ethical evaluation of surveillance systems that involves (i) initial policies, procedure, and capabilities of the surveillance systems; (ii) characteristics of surveillance tools; (iii) goals of the system; (iv) fitness between means and goals of the system; (v) data collection and analysis involved in the system; (vi) rights and resources of the surveillance subjects; and (vii) protection and fate of the collected data.

These concepts are extended by Haemmerli et al. in Chapter 2, "Trust Networks among Human Beings: Analysis, Modeling, and Recommendations," where the authors analyze the issues related to the problem of trust in worldwide connected networks (like the Internet), providing basic definitions, reference models, and practical guidelines for trust development. The chapter also stresses the importance of taking into account cultural diversities and national laws, surveying current frameworks and tools.

In Chapter 3, "Art of Balancing Utilities: Privacy and Video Surveillance in Sweden," Björklund discusses how public video surveillance systems have been finding increasing deployments, with relatively less concern being shown by the public on its associated privacy violation issues. The author argues that the Swedish approach toward homeland security may be described as consistently utilitarian and as a manifestation of a proactive welfare state legacy.

The same topic is addressed by Leese in Chapter 4, "Perceived Threat: Determinants and Consequences of Fear of Terrorism in Germany," presenting the results of a survey conducted in Germany on "fear of terrorism." The study shows that there is an increasing shift in the citizen's mind from the issues of civil liberties to acceptance of different security and surveillance measures introduced by the Government of Germany for prevention of any attack.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Moving a step toward the optimal trade-off between security and privacy, Paruchuri et al., in Chapter 5, "Preserving and Managing Privacy Information in Video Surveillance Systems," propose a privacy-preserving video surveillance system that can help to protect privacy-sensitive information by using a rate-distortion optimized data-hiding scheme. This scheme allows retrieval of private data with a robust, yet anonymous, authentication module that utilizes encrypted biometric signals.

A very similar topic is further investigated in Chapter 6, "Objective and Subjective Evaluation of Content-Based Privacy Protection of Face Images in Video Surveillance Systems Using JPEG XR," where Sohn et al. use both objective and subjective assessments to analyze the level of privacy protection achieved by a layered scrambling technique, developed by the authors for video surveillance systems. Experimental results have been analyzed to show and judge the strength of privacy protection provided by different approaches for different use cases.

Part II: Physical and Cyber Surveillance

In the cyberphysical surveillance framework, the very first element is the capability of the system to detect events of interest. The issue is described by Atrey in Chapter 7, "Event Representation in Multimedia Surveillance Systems." The framework proposed by the author defines events at three levels of a hierarchical structure: transient, atomic, and compound. The events at the lower level are mapped into those at the higher ones by a clustering technique. The framework also analyzes the relationships between various events from three dimensions: temporal, causal, and spatial.

In Chapter 8, "Challenges and Emerging Paradigms for Augmented Surveillance," Flammini et al. identify several components of "augmented surveillance systems," such as (i) improved sensor technology; (ii) use of combined and diversified sensing technologies, leading to multimodal distributed surveillance; and (iii) proactive and early detection of events by superior situation awareness and decision support capabilities. The authors also describe how such an augmented surveillance system can be realized in practice and deployed in real world.

In Chapter 9, "Pervasive Surveillance System Management," Hilal and Basir discuss the various issues and challenges in designing sensor-based intelligent systems management framework for carrying out a pervasive and ubiquitous surveillance operation. The authors present a detailed survey on the state-of-the-art sensor management architectures and strategies for deployment in real-world surveillance systems.

How information collected by sensors can be merged in order to assess the actual situation and to predict near-future evolution is addressed by Digioia et al. in Chapter 10, "Moving from Measuring to Understanding: Situation Awareness in Homeland Security." This chapter presents a critical review of various existing methodologies and schemes for fusion of data from multiple and heterogeneous sources to obtain a high-level pattern, or behavior detection and prediction, and to achieve situational awareness in the context of homeland security. The authors have also discussed some popular and widely used mechanisms for extraction of high-level information from raw data gathered by heterogeneous sensors.

In Chapter 11, "Ergonomic Design and Evaluation of Surveillance Systems," Coelho and Nunes present the ergonomical and human-related factors in designing surveillance systems. The authors present a survey on the various human factors for achieving an effective human–system coupling in a surveillance system, with particular attention on perception and modes of control, as well as on information processing. The authors also focus on an evaluation framework for surveillance systems based on ergonomic considerations, such as usability and user-centered design, as well as from an operational efficiency perspective.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Moving to the cyberspace domain, whose surveillance is nowadays essential to prevent possibly disruptive cyberattacks, in Chapter 12, "Awareness, Assessment, and Reduction of Web Application Vulnerability," Ward and Cavestro analyze the threats in the World Wide Web, which are especially important when these applications are used in business-critical domains (e.g., finance). The chapter also presents the future trends in web applications and the related societal and legislative issues.

In Chapter 13, "Distributed Framework for Cybersecurity of Critical Infrastructures," D'Antonio et al. present various challenges in detecting different attacks in SCADA network systems. The identification of potential attacks requires that the information is gathered from several different sources and diverse geographical locations, and there are no general locality principles that can be gainfully applied for detecting such attacks. The authors also propose a distributed framework for SCADA system security, which consists of a number of modules whose operations are integrated and coordinated in unison, so as to achieve overall protection of the SCADA system itself.

In Chapter 14, "Modeling and Counteracting Virus Diffusion in Sensor Networks for Net-Centric Surveillance Systems," Battistelli et al. discuss the issue of the adverse impact of malicious viruses and other malwares on the operations of surveillance systems based on wireless sensor networks. The authors present a detailed study on various models for virus diffusion, and their detrimental effects on network connectivity, and other network operations. Simulation results are presented to show how the spreading of virus affects in-network information fusion, causing serious disruption in monitoring activities.

Part III: Technologies for Homeland Security

In the context of developing software solutions for homeland security applications, Chapter 15, "GEPSUS GEOINT Applications for Homeland Security," by De Amicis et al., addresses the important roles being played by geospatial technologies. As a specific case study, the authors present the details of the project GEPSUS (Geographical Information Processing for Environmental Pollution-Related Security within Urban Scale Environments) to show how geographical intelligence (GEOINT) technologies can significantly help in designing solutions for enhancing the security of humans and infrastructures against human-launched or natural disasters. The chapter also illustrates a simulation framework for natural emergencies such as landslides, floods, and human-made disasters such as intentional release of toxic and poisonous gases.

In Chapter 16, "Omnidirectional Human Intrusion Detection System Using Computer Vision Techniques," Wong et al. discuss how a system can be designed to detect human intrusions using the techniques of computer vision. The authors defined such a system as "omnidirectional," since it is capable of carrying out surveillance over a full area under its coverage, without leaving any blind spot. For designing a system of this kind, the authors have used vision spectrum and infrared imaging: in particular, for intrusion detection, a "partitioned region of interest" algorithm and a "human head curve" algorithm are utilized.

In Chapter 17, "Wireless Sensor Networks and Audio Signal Recognition for Homeland Security," Martalò et al. propose a security solution using audio signal pattern recognition techniques over a wireless sensor network. The authors propose a signal pattern recognition mechanism based on a simple time-domain approach, and they show how this approach can be utilized in a commercial application using unattended ground sensors. The mechanism is further enhanced by using a hybrid time-frequency approach for achieving higher accuracy in the results.

In Chapter 18, "Dynamic Bayesian Multitarget Tracking for Behavior and Interaction Detection," Marcenaro et al. propose the use of a joint human tracking and human-to-human

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

interaction recognition system in video surveillance. Although effective tracking is a fundamental building block for video analytics in surveillance applications, it is challenging to design tracking algorithms that effectively operate in crowded public places. The proposed tracking algorithm recursively works between time slices and makes use of a forward–backward message passing within each time slice under a probabilistic graphical model framework.

In Chapter 19, "Imaging Tunnels and Underground Facilities Using Radio-Frequency Tomography," Lo Monte et al. present a discussion on the surveillance mechanism of targets, which are hidden such as under a tree, inside a building, or below the ground. The authors argue that the design of underground imaging facilities is of critical importance for the protection of international borders and sensitive areas. For achieving effective remote sensing and detection of events, the authors propose radio-frequency, tomography-based remote sensing that utilizes randomly deployed transceivers, which communicate with base stations over the ground, in case the anomaly is detected underground.

In Chapter 20, "Surveillance Framework for Ubiquitous Monitoring of Intermodal Cargo Containers," Varma et al. discuss various issues in designing a global seamless cargo monitoring system and present relevant protocols and existing standards for this purpose. The authors also propose a framework for containerized cargo monitoring system, which integrates the existing resources for container monitoring with advanced geospatial threat detection using global data. This framework is particularly relevant in today's world since the security of ports and intermodal cargo containers is essential for protecting nations against potential threats of terrorism.

Finally, in Chapter 21, "Model-Based Control of Building Evacuation Using Feedback from Sensor and Actuator Wireless Networks," Lino et al. focus their attention on an important issue related to human security—safe evacuation of a large number of humans from buildings or open-air environment—in the event of an attack or an unforeseen incident. The authors propose a supervisory model-based controller for designing an evacuation system, operating on the data coming from a distributed sensor network. The control actions of the system are coordinated to reduce the human egress time so that safe dynamics of the crowd are guaranteed.

Francesco Flammini
Roberto Setola
Giorgio Franceschetti
Editors

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Acknowledgment

The editors would like to warmly thank all the outstanding experts, serving as chapter authors and/or members of the editorial board, who have contributed to make this book an essential reference source in its area.

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Editors

Francesco Flammini got with honors his laurea (2003) and doctorate (2006) degrees in computer engineering from the University of Naples Federico II. Since October 2003, he has worked in Ansaldo STS (Finmeccanica) on the safety and security of rail-based transportation infrastructures. He has taught computer science and software engineering as an adjunct professor at the University of Naples, as well as seminars on computer dependability and critical infrastructure protection in postdegree courses on homeland security. He has coauthored several books and more than 50 scientific papers published in international journals and conference proceedings. He has served as the chairman, a PC member, and an editor for several international conferences and journals. He is a senior member of the IEEE, an ACM Distinguished Speaker, and the vice-chair of the IEEE Computer Society Italy Chapter. He is also member of the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS TC7), FME (Formal Methods Europe), ERCIM WG on Formal Methods for Industrial Critical Systems (FMICS), ESRA TC on Operational Safety & Security of Interconnected Critical Infrastructures, and IEEE SMC TC on Homeland Security.

Roberto Setola obtained his master of science in electronic engineering (1992) and PhD in electronic engineering and computer science (1996) from the University of Naples Federico II. He currently serves as a professor of automatic control at University CAMPUS BioMedico and head of the COSERITY Lab (Complex Systems & Security Lab). He is also the director of the master's program for "Homeland security, systems and methods and tools for security and crisis management." Formerly a member of the Italian Prime Minister's Office (1999–2004), Setola was the coordinator of the working group on critical information infrastructure protection established by the Italian Prime Minister (2003–2004), a member of the G8 Senior Expert CIIP Group (2002–2006), and an affiliate of the G8 working group on High-Tech Crime (2002–2004). Since 1992, Roberto, in collaboration with several universities and research centers, has presented numerous studies on many topics related to modeling, simulation, and control of complex networks and systems and the protection of critical infrastructures. In addition, he has been the coordinator of the EU DG JLS project SecuFood on the security of the food supply chain and coordinator of the EU DG HOME project FACIES on the automatic identification of failure/attack in critical infrastructures. Moreover, as leader of a specialized unit, Setola was involved in more than 12 national and international projects related to critical infrastructure protection and homeland security. Throughout his career, Roberto has coauthored

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

3 books, edited 3 books, been a guest editor of 3 special issues on international journals, been an editor in chief of 2 magazines, and coauthored roughly 130 scientific publications. Setola is a founding member and current general secretary of the "AIIC—Associazione Italiana esperti in Infrastrutture Critiche", senior member of the IEEE, and founding member of the IFIP 11.10 working group on critical infrastructure protection.

Giorgio Franceschetti is emeritus professor, University of Naples Federico II, and distinguished visiting scientist, JPL. He has been adjunct professor, UCLA (1992–2008), visiting professor in many European and U.S. universities, and lecturer in China, India, and Somalia. He is the author of 12 books and of about 200 papers in international journals of recognized standard in the area of basic and applied electromagnetic theory, remote sensing, signal processing, and homeland security. He is also a life fellow of the IEEE and member of the Electromagnetic Society. Among many outstanding awards, he is recipient of the Gold Medal of the Italian Republic President (2001); the Marconi (1975), Philip Morris (1990), IEE London Mountbatten (1998), and IEEE AP-Society (1999 and 2008) Schelkunoff Prizes; and the IEEE GRS-Society (2007), the NASA Cassini Radar Team (2009), and the IEEE APS-Society (2010) Distinguished Achievement Awards. As honorary positions, he has been appointed Officer of the Italian Republic (2003) and Bruno Kessler Honorary Chair, University of Trento, Italy (2010).

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Contributors

Pradeep K. Atrey
Department of Applied Computer Science
University of Winnipeg
Winnipeg, Manitoba, Canada

Ronald D. Barnes
School of Electrical and Computer Engineering
University of Oklahoma
Norman, Oklahoma

Otman A. Basir
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada

Giorgio Battistelli
University of Florence
Florence, Italy

Fredrika Björklund
School of Social Sciences
Södertörn University
Huddinge, Sweden

Jessica Cavestro
Jessoftware
Fontaneto, Italy

Sen-Ching S. Cheung
Department of Electrical and Computer Engineering
University of Kentucky
Lexington, Kentucky

Luigi Chisci
University of Florence
Florence, Italy

Michał Choraś
ITTI Sp. z o.o.
Poznań, Poland

and

Institute of Telecommunications
University of Technology and Life Sciences
Bydgoszcz, Poland

Denis A. Coelho
Department of Electromechanical Engineering
University of Beira Interior
Covilha, Portugal

Giuseppe Conti
Fondazione Graphitech
Trento, Italy

Luigi Coppolino
Department of Technology
University of Naples "Parthenope"
Naples, Italy

Salvatore D'Antonio
Department of Technology
University of Naples "Parthenope"
Naples, Italy

Raffaele De Amicis
Fondazione Graphitech
Trento, Italy

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Wesley De Neve
Department of Electrical Engineering
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea

Alberto Debiasi
Fondazione Graphitech
Trento, Italy

Giusj Digioia
University of Roma Tre
Rome, Italy

Danilo Erricolo
University of Illinois at Chicago
Chicago, Illinois

Alfonso Farina
Selex Electronic Systems S.p.A.
Rome, Italy

Gianluigi Ferrari
Department of Information Engineering
University of Parma
Parma, Italy

Francesco Flammini
Ansaldo STS
Naples, Italy

Chiara Foglietta
University of Roma Tre
Rome, Italy

Giorgio Franceschetti
University of Naples Federico II
Naples, Italy

Antonio Graziano
Selex Electronic Systems S.p.A.
Rome, Italy

Bernhard Haemmerli
Gjovik University College, Norway
Lucerne, Switzerland

Allaa R. Hilal
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada

Rafał Kozik
ITTI Sp. z o.o.
Poznań, Poland

and

Institute of Telecommunications
University of Technology and Life Sciences
Bydgoszcz, Poland

Dohyoung Lee
Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario, Canada

Matthias Leese
Section Security Ethics
International Centre for Ethics in the Sciences and Humanities
University of Tuebingen
Tuebingen, Germany

Alessio Liburdi
Selex Electronic Systems S.p.A.
Rome, Italy

Way Soong Lim
Faculty of Engineering and Technology
Multimedia University
Melaka, Malaysia

Paolo Lino
Department of Electrical and Electronics Engineering
Technical University of Bari
Bari, Italy

Lorenzo Lo Monte
University of Dayton Research Institute
Dayton, Ohio

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Chu Kiong Loo
Faculty of Computer Science and Information Technology
University of Malaya
Kuala Lumpur, Malaysia

Ying Luo
Department of Electrical and Computer Engineering
University of Kentucky
Lexington, Kentucky

Daniele Magliocchetti
Fondazione Graphitech
Trento, Italy

Bruno Maione
Department of Electrical and Electronics Engineering
Technical University of Bari
Bari, Italy

Guido Maione
Department of Electrical and Electronics Engineering
Technical University of Bari
Bari, Italy

Claudio S. Malavenda
Selex Electronic Systems S.p.A.
and
Sapienza University of Rome
Rome, Italy

Lucio Marcenaro
Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture
University of Genova
Genoa, Italy

Marco Martalò
School of Engineering
E-Campus University
Novedrate, Italy

and

Department of Information Engineering
University of Parma
Parma, Italy

Gary T. Marx
Department of Urban Studies and Planning
Massachusetts Institute of Technology
Cambridge, Massachusetts

Giovanni Mugnai
University of Florence
Florence, Italy

Konstantinos N. Plataniotis
Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario, Canada

Isabel L. Nunes
Faculdade de Ciências e Tecnologia
Department of Mechanical and Industrial Engineering
University Nova de Lisboa
Caparica, Portugal

Gabriele Oliva
Complex Systems and Security Laboratory
Campus Bio-Medico University
Rome, Italy

Stefano Panzieri
University of Roma Tre
Rome, Italy

Alfio Pappalardo
Ansaldo STS
Naples, Italy

and

University of Naples Federico II
Naples, Italy

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)

Jithendra K. Paruchuri
Department of Electrical and Computer Engineering
University of Kentucky
Lexington, Kentucky

Stefano Piffer
Fondazione Graphitech
Trento, Italy

Federico Prandi
Fondazione Graphitech
Trento, Italy

Margrete Raaum
Gjøvik University College
Gjøvik, Norway

Carlo S. Regazzoni
Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture
University of Genova
Genoa, Italy

Yong Man Ro
Department of Electrical Engineering
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea

Roberto Setola
Complex Systems and Security Laboratory
Campus Bio-Medico University
Rome, Italy

Andrej Škraba
University of Maribor
Kranj, Slovenia

Hosik Sohn
Department of Electrical Engineering
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea

Francesco Soldovieri
Consiglio Nazionale delle Ricerche
Rome, Italy

Mauricio Soto
Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture
University of Genova
Genoa, Italy

Radovan Stojanović
University of Montenegro
Podgorica, Montenegro

Diego Taglioni
Fondazione Graphitech
Trento, Italy

Monte Tull
School of Electrical and Computer Engineering
University of Oklahoma
Norman, Oklahoma

Yogesh Varma
School of Electrical and Computer Engineering
University of Oklahoma
Norman, Oklahoma

Valeria Vittorini
University of Naples Federico II
Naples, Italy

David Ward
Security Technology Assessment Unit
Joint Research Centre
Ispra, Italy

Michael C. Wicks
University of Dayton Research Institute
Dayton, Ohio

Wai Kit Wong
Faculty of Engineering and Technology
Multimedia University
Melaka, Malaysia

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Edited by Francesco Flammini, Roberto Setola, and Giorgio Franceschetti
International Standard Book Number-13: 978-1-4398-8324-2 (Hardback)