7. PRIVACY VERSUS NATIONAL SECURITY
Clarifying the Trade-off

JENNIFER CHANDLER

I. The Meaning of "Privacy" and "Security" in the Privacy Versus Security Trade-off 122
- A. Security 123
- B. Privacy 124

II. Explaining the "Weight" of Security 125
- A. Is Security the Prime Value? 126
- B. Human Perception of Risk 127
- C. Inherent Limits to the Value of Privacy 128
- D. The Distributive Implications of Counterterrorism 129
- E. A Social Psychological Need for a Reaction 131
- F. Courts and the Security Versus Privacy Trade-off 131

III. Reframing the Trade-Off: Security Versus Security 132
- A. Security Theatre 132
- B. Security Measures May Introduce New Vulnerabilities 133
- C. Security Measures May Reduce the Security of a Minority of the Population 135

IV. Conclusion 137

After the September 11 attacks, the idea that civil liberties had to be reduced in favor of national security emerged with renewed vigor. Many have noted the paradox that security measures intended to protect a liberal democracy can end up eroding the civil liberties at the heart of that liberal democracy.[1] It is common to view this problem as one of striking the appropriate balance or trade-off between security and civil liberties.[2] The focus of this chapter is on an aspect of this general problem, namely the trade-off between privacy and national security.

1. See Jef Huysmans, "Minding Exceptions: The Politics of Insecurity and Liberal Democracy," *Contemporary Political Theory* 3 (2004): 321 at 322.

2. Richard Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency*, (New York: Oxford University Press, 2006); Eric A. Posner and Adrian Vermeule, *Terror in the Balance: Security, Liberty and the Courts* (New York: Oxford University Press, 2007); Kent Roach, "Must we trade rights for security? The choice between smart, harsh or proportionate security strategies in Canada and Britain," *Cardozo Law Review* 27 (2005–2006): 2151; Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003); Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy* 11 (2003): 191; K. A. Taipale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy

The need for a trade-off between privacy and security is likely true in certain contexts and with respect to certain aspects of the right to privacy. However, framing the issue as a contest between privacy and national security tends prematurely to shut down the debate in favor of security.[3] Security has been described as the "trump of trumps," outweighing civil and political rights.[4]

However, the danger with prematurely permitting the needs of national security to trump competing values is that important questions may not be adequately considered. These include

1. Whether the contemplated security measure actually delivers any security
2. Whether there is a less privacy-invasive manner to achieve the same level of security
3. Whether the gains in security are worth the total costs of the security measure, including privacy costs and the opportunity costs of security-enhancing spending on health, education, poverty, and the environment
4. Whether the costs are distributed fairly so that the increased security of the majority is not purchased by sacrificing the interests of a minority

If the security versus privacy trade-off is biased in favor of security, particularly in times of public insecurity, there is reason to fear that we may too easily sacrifice rights and freedoms such as privacy. One of the difficulties is in trying to balance two different values against one another. As a result, this chapter proposes a reframing strategy designed to highlight some of the ways that privacy-reducing counterterrorism measures also reduce security. In this way, at least some measure of protection for privacy may be achieved by analyzing the trade-off as one of security versus security.

I. THE MEANING OF "PRIVACY" AND "SECURITY" IN THE PRIVACY VERSUS SECURITY TRADE-OFF

The privacy versus security trade-off is often asserted to be an unavoidable, if lamentable, necessity. It is rare that the meaning of the terms is made clear, or that the process of balancing them is explained. Below, I sketch out the meaning of the terms "privacy" and "security," with emphasis on the points that will shed light on the nature of the trade-off between the two.

---

and the Lessons of King Ludd," *Yale Journal of Law & Technology* 7 (2004–2005): 123; Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999); Jeffrey Rosen, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror," *Arizona Law Review* 46 (2004): 607.

3. Peter P. Swire, "Privacy and Information Sharing in the War on Terrorism," *Villanova Law Review* 51 (2006): 101 at 124–125.

4. Conor Gearty, "Reflections on Civil Liberties in an Age of Counterterrorism," *Osgoode Hall Law Journal* 41 (2003): 185 at 204–5.

A. Security

Security has been defined as an "absence of threats to acquired values"[5] or a "low probability of damage to acquired values."[6] A distinction is often drawn between objective and subjective security. Objective security refers to the low probability of damage, while subjective security refers to the feeling of security, or the absence of fear that acquired values are threatened.[7] The subjective component of security is highly relevant in the context of terrorism, which works primarily by inducing fear rather than by posing a real physical threat to most people.

While one can have objective without subjective security (or the reverse), the two are related. It is possible that an incorrect subjective perception of risk may become an actual threat to objective security. This is because fear may produce counter-productive risk avoidance or destabilize society. On the other hand, an absence of justified fear may cause a person to run greater objective risks, with the same holding true at the national level. Security may thus require that one be objectively free from risk and also subjectively feel free from risk.

The above-mentioned definition of security is very general. It does not specify the entity whose security is at issue (e.g., the individual, a group, the state, the international system, or the biosphere[8]) or the types of values amenable to being secured. During the 1980s, the concept of security in political science was broadened beyond a concern with the security of the state (national security), which entailed a focus on international relations and military issues, toward the security of people as individuals or as collectivities.[9] The security of people ("human security") is understood to extend beyond national security, also including economic welfare, the health of the environment, cultural identity, and political rights.[10] Thomas suggests that human security incorporates both quantitative and qualitative aspects. The quantitative aspect refers to the satisfaction of the basic material needs essential for survival, including food, shelter, and health care, while the qualitative aspect refers to "the achievement of human dignity which incorporates personal autonomy, control over one's life, and unhindered participation in the life of the community."[11]

---

5. Arnold Wolfers, "National Security as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (1952): 481 at 485.

6. David A. Baldwin, "The Concept of Security," *Review of International Studies* 23 (1997): 5 at 13.

7. Wolfers, "National Security," (n. 5) at 485; Lucia Zedner, "The Pursuit of Security," in *Crime Risk and Security*, eds. Tim Hope and Richard Sparks (London: Routledge, 2000) 200 at 202.

8. Emma Rothschild, "What is security?" *Daedalus* 124, no. 3 (1995): 53 at 55; Baldwin, "Concept of Security," 13 (n. 6).

9. Ole Waever, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz, (New York: Columbia Univ. Press, 1995), 47.

10. *Ibid.*, 47.

11. Caroline Thomas. Global Governance, Development and Human Security. (London: Pluto Press, 2000), 6–7.

When we are considering the trade-off between "privacy" and "security," should we adopt a narrow or broad concept of security? Most discussions of the trade-off after September 11 have contemplated security in a narrower sense than that meant by "human security." The pursuit of security in this context has most often been understood to be counterterrorist efforts intended to defend the physical security of people and property as well as the stability of the state, and the following analysis will adopt this concept of security.

B. Privacy

The nature and moral significance of "privacy" are difficult questions that have attracted significant philosophical attention.[12] There is disagreement over whether "privacy" actually refers to something fundamental and coherent or simply groups together diverse issues that have a superficial connection.[13] Accepting that the concept of privacy is a coherent and useful one, various writers have proposed definitions of privacy. It has been variously described as a person's claim to determine what information about him or herself is communicated to others, a person's measure of control over personal information and over who has sensory access to him or her, and a state or condition of limited access to the person.[14]

Although these descriptions assist in identifying the nature of privacy, it is still necessary to explain why it should or should not be protected. Here again, there are various explanations of why privacy is important. Privacy is said either to promote or to be a necessary component of human interests of inherent value such as human dignity, autonomy, individuality, liberty, and social intimacy.[15] A person who is completely subject to public scrutiny will lose dignity, autonomy, individuality, and liberty as a result of the sometimes strong pressure to conform to public expectations.[16] In addition to freedom from the pressure to conform, privacy also protects the individual from another party's use of his or her information to manipulate, out-compete, or otherwise exploit the individual.

The value of privacy takes on another dimension as a result of modern information technologies. A certain measure of privacy with respect to personal information used to be ensured by the technological limits on its storage,

12. Allan Westin, *Privacy and Freedom* (New York: Atheneum, 1967); Ruth Gavison "Privacy and the Limits of Law," *Yale Law Journal* 89 (1980): 421 at 424.

13. Ferdinand Schoeman, "Privacy: Philosophical Dimensions of the Literature," in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. Schoeman (New York: Cambridge Univ. Press, 1984) at 5.

14. *Ibid*, at 2–3; Gavison, "Privacy," 428 (n. 12).

15. Schoeman, "Privacy: Philosophical Dimensions," (n. 13) at 8; Gavison, "Privacy," 448–55 (n. 12); James Rachels, "Why Privacy is Important" *Philosophy and Public Affairs* 4, no. 4 (1975): 323.

16. Schoeman, "Privacy: Philosophical Dimensions," 19 (n. 13); Gavison, "Privacy", 448 (n. 12).

communication, and cross-referencing with other information. However, as information technology has become more sophisticated and efficient, it has become possible to collect and integrate large quantities of personal information. "Data surveillance" or "dataveillance" refers to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.[17] The systematic collection, from multiple sources, of large quantities of personal information creates risks for individuals. While the risks mentioned in the preceding paragraphs flow from the disclosure of true and relevant information about an individual, dataveillance creates the additional risk that incorrect or unreliable data may come to be used to make judgments about whether to apply benefits or sanctions to individuals. In addition, as databases are integrated, data that was sufficiently reliable and relevant in one context may come to be used for inappropriately sensitive purposes.

Westin suggests that there are two main sources of social pressure against individual privacy. The first is human curiosity or the seemingly universal "tendency on the part of individuals to invade the privacy of others."[18] Second, and more applicable in this context, is the use of surveillance "to enforce the rules of the society."[19] Since terrorism (particularly suicide terrorism) is not easily deterred by punishment after the fact, the pressure to detect and preempt terrorist plots is strong. Increased surveillance is therefore a predictable response to a dramatic terrorist attack.

II. EXPLAINING THE "WEIGHT" OF SECURITY

The purpose of this section is to consider why security is so powerful, and why it seems fairly easily to trump competing values such as privacy. The reasons suggested for security's rhetorical power are first that security in the sense of physical survival is a prerequisite for the enjoyment of other values such as privacy.[20] Second, human risk perception may be subject to cognitive biases that cause us to overestimate the risk of terrorism and to have difficulty perceiving the harm of reduced privacy. Third, we are apt to think that it is better to have more rather than less security, while this is not true for privacy. Fourth, to the extent that national security is obtained at the expense of the privacy of a minority,

17. Roger Clarke, "Dataveillance: Delivering '1984'" in *Framing Technology: Society, Choice and Change* eds. L. Green and R. Guinery (Sydney: Allen & Unwin, 1994), available at www.anu.edu.au/people/Riger.Clarke/DV/PaperPopular.html.

18. Westin, *Privacy and Freedom*, 19 (n. 12).

19. *Ibid.*, 20.

20. Although some values may be protected beyond death (e.g., autonomy rights dictate respect for an individual's expressed wishes with respect to the use of his or her remains), the full enjoyment of these values exists during life.

the majority is more likely not to perceive or care about the privacy costs and thus will regard the security measures as reasonable. Fifth, social-psychological reactions of solidarity following an external attack may cause people to be more willing to set aside individual rights claims such as privacy for a perceived collective benefit in terms of national security. Finally, judges tend to defer to governments on matters of national security.

A. Is Security the Prime Value?

Security is privileged over values such as liberty and autonomy in various strands of political philosophy, with an important role of the state being the protection of the physical security of people and property. This is so in competing individualistic and communitarian accounts of the state. The idea of the social contract has been an important part of western political philosophy for centuries, serving to justify political authority. Classical social contractarians emphasized the dangerousness of life in the "state of nature."[21] The social contract was the means by which people voluntarily surrendered a certain measure of their individual freedom in exchange for the security and protection provided by a legitimate political authority. According to these views, security is a primary obligation of the state since that is what individuals have contracted for in submitting to state authority. The communitarian perspective also privileges security over individual privacy.[22]

Baldwin refers to this approach to valuing security as the "prime value" approach, and challenges it by suggesting that it is logically and empirically indefensible.[23] The prime value approach would suggest that all societal resources should be poured into the pursuit of absolute security. As an empirical matter, we do not behave in this way. It is unfortunately clear that even affluent societies do not value the survival of their members above all else. For example, no society puts all of its resources into health care, and the resulting underfunding indirectly takes lives. Instead, each society chooses a level of basic security, which may not entail survival for all its members, and allocates the remaining resources to other values according to the relative importance of those values to that society.

If we pursue neither absolute security, nor the level of security required to ensure basic survival for everyone, it does not make sense to say that security is the prime value or that it ought necessarily to trump values such as liberty or privacy. One response to this argument is that we may be willing to make compromises between the various values essential to survival, but that we would not trade a survival requirement for a nonsurvival value such as privacy. In other words, we would spread resources between health care, housing, nutrition and

21. David Boucher and Paul Kelly eds, *The Social Contract From Hobbes to Rawls* (London: Routledge 1994), 2–10.

22. Etzioni, *The Limits of Privacy*, 42 (n. 2).

23. Baldwin, "Concept of Security," 18 (n. 6).

counterterrorism (for example), even though we could not assure a basic level of any of these goods for all members of society, but we would not underfund any of these survival requirements in order to obtain liberty or privacy.

In the end, it is probably true that, up to a point, we view survival as more important than the protection of fundamental rights and freedoms that we feel are essential to a good life. This cannot be taken so far that the life being secured is no longer felt to be worth living because it is without liberty, privacy, or other rights. However, the sacrifice of privacy for security in the context of counterterrorism measures has not reached this stage for the general public. As a result, it is possible that the view that survival is indispensable for the full enjoyment of civil liberties is partly responsible for the greater weight accorded to security over privacy after September 11.

B. Human Perception of Risk

Research in the psychology of risk perception suggests that people employ a set of heuristics to assess probabilities, and that these heuristics can produce serious and persistent biases.[24] Some of these tendencies lead people to overestimate the risks of terrorism. At the same time, they cause people to be relatively unconcerned about the risks to privacy caused by counterterrorist security measures.

The "availability heuristic" refers to the tendency of people to assess the probability of an event by the ease with which occurrences can be brought to mind by recall or imagination.[25] Familiar, recent, or salient events seem more probable because they are more available to the mind than the less famous, older, or less dramatic events.[26] Similarly, whether a risk can be easily imagined or not also affects assessments of its probability.[27] An important consequence of the availability heuristic is that repeated discussion, for example in the media, of a low-probability hazard will increase its perceived riskiness regardless of the actual probability of harm.[28] The harms of terrorism are famous, dramatic, recent, vividly imaginable, and repeatedly covered in the media. On the other hand, the consequences of counterterrorism measures for civil liberties are much less available to the mind and so tend not to evoke as much concern.

---

24. Paul Slovic, "Perception of Risk" (1987) reprinted in Paul Slovic, *The Perception of Risk*, (London: Earthscan Publications Ltd, 2000) 220, at 221–222; Amos Tversky and Daniel Kahneman, "Judgment Under Uncertainty: Heuristics and Biases," (1974) reprinted in *Judgment Under Uncertainty: Heuristics and Biases*, eds. Kahneman, Slovic, and Tversky (Cambridge: Cambridge Univ. Press 1982), 3.

25. Tversky and Kahneman, "Judgment Under Uncertainty," 11 (n. 24).

26. *Ibid.*, 11.

27. *Ibid.*, 12–13.

28. Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Facts Versus Fears: Understanding Perceived Risk," in *Judgment Under Uncertainty: Heuristics and Biases*, eds. Kahneman, Slovic, and Tversky (Cambridge: Cambridge Univ. Press 1982), 463.

In addition to the consequences of the "availability heuristic," terrorism also pushes "all the risk perception hot buttons" since it has "vivid and dreadful consequences; exposure is involuntary and difficult to control (or avoid); and it is unfamiliar, often catastrophic, and caused by human malevolence."[29] Risks of this type are termed "dread risks."[30] People are more apt to avoid dread risks than risks in which a similar or greater number of people are killed over a longer period of time.[31]

People also tend to be insensitive to probability with respect to strongly positive or negative events.[32] They tend to react to the possibility rather than the probability of the event, which causes very small probabilities to carry great weight.[33] Slovic suggests that this cognitive distortion is particularly at issue with terrorism.[34]

C. Inherent Limits to the Value of Privacy

Another reason why security seems to be a more compelling value than privacy is perhaps that privacy is an inherently limited value, while security is not. As a result, we are more likely to always want more security, but unlikely to feel the same way about privacy.

Most individuals want an intermediate level of privacy, rather than complete exposure to or complete isolation from others.[35] As Gavison writes, "Privacy thus cannot be said to be a value in the sense that the more people have of it, the better."[36] Indeed, some of the justifications for privacy inherently contemplate that privacy is not to be an absolute insulation of the individual from all others. For example, it is said that without privacy we would be unable to form close relationships since the relinquishment of some privacy to selected people is a critical aspect of how we form closer and deeper relationships.[37] If everyone knew everything about us, these gradations of closeness would be more difficult to establish. However, if everyone knew nothing about us, we similarly would be unable to establish close relationships.

---

29. Paul Slovic, "What's fear got to do with it? It's affect we need to worry about." *Missouri Law Review* 69 (2004): 971 at 985.

30. Slovic, "Perception of Risk" (n. 24) at 225.

31. Gerd Gigerenzer, "Out of the Frying Pan into the Fire: Behavioral Reactions to Terrorist Attacks," *Risk Analysis* 26, no. 2, (2006): 347 at 347.

32. Slovic, "What's fear got to do with it?" (n. 29) at 982.

33. *Ibid.*

34. *Ibid.*, 987.

35. Westin, Privacy and Freedom, 7 (n. 12).

36. Gavison, "Privacy," 440 (n. 12).

37. Emanuel Gross, "The struggle of a democracy against terrorism—Protection of human rights: The right to privacy versus the national interest—The proper balance," *Cornell International Law Journal* 37, (2004): 27 at 32.

The goal of security is not subject to the same type of inherently desirable limits. It may be that we unconsciously have an ambivalent attitude toward privacy, while we are more certain that more security is a good thing.

D. The Distributive Implications of Counterterrorism

Another of the reasons why security may trump privacy in the context of counterterrorism is that the security improvement is sometimes bought at the expense of a minority. To the extent that this is true, the majority will either fail to perceive the costs of that security or they will not care sufficiently. As will be discussed further below, the "war on terror" exposes Muslims and those of Arab ethnicity to increased risks of being falsely suspected of terrorism and mistreated.[38]

To the extent that we obtain objective or subjective security at the expense of a minority, there is distributive injustice. However, the distributive implications of counterterrorism measures are not so clear. One must consider both who is at greater risk because of counterterrorism measures, as well as who is at greatest risk of harm from terrorism if an effective counterterrorism measure is not adopted.

The groups most at risk from a terrorist attack vary according to the type and location of the attack. It may be that the failure to take effective counterterrorism measures may disproportionately harm disadvantaged minorities within the population. If this is true, counterterrorism efforts may disproportionately both help and harm different vulnerable minorities.

The majority of the victims in the September 11 attack on the World Trade Center were Caucasian men living in the United States.[39] Other types of terrorist targets may disproportionately affect other groups of people. The population at risk of an attack on public transportation in the United States is different, where users of public transport are less than 50% Caucasian and male, and are likely to have a lower than average household income.[40] Industrial plants are another type of potential target for terrorist attacks,[41] and members of disadvantaged

38. CAIR-Canada, "Presumption of Guilt: A National Survey on Security Visitations of Canadian Muslims," (8 June 2005), http://www.caircan.ca/downloads/POG-08062005.pdf at 3.

39. "Demographic Data on the Victims of the September 11, 2001 Terror Attack on the World Trade Center, New York City," *Population and Development Review* 28, no. 3 (2002): 586.

40. John Neff and Larry Pham, American Public Transportation Association, "A Profile of Public Transportation Passenger Demographics and Travel Characteristics Reported in On-Board Surveys" (May 2007), http://www.apta.com/government_affairs/policy/documents/transit_passenger_characteristics_07.pdf.

41. Thomas C. Beierle, "The Benefits and Costs of Disclosing Information About Risks: What do We Know about Right-to-Know?" *Risk Analysis* 24, no. 2 (2004): 335.

groups disproportionately live near hazardous industrial installations.[42] To the extent that terrorism targets these industrial plants, the victims would come disproportionately from within the disadvantaged groups within society.

Disadvantaged segments of the community are also more vulnerable to harm in the event of a disruption of critical public infrastructures. In the aftermath of Hurricane Katrina, it was seen that poor and racialized persons suffered the most from the disruption.[43]

Terrorism also poses the risk of revenge attacks and discrimination, depending upon the nature of the terrorist attack. After September 11, many people of Arab (and Arab-appearing) ethnicity were subject to a sharply increased level of hate crimes.[44] Unfortunately, this community might suffer a disproportionate risk of being targeted for revenge attacks should counterterrorism measures not successfully stop further attacks or should the public's feeling of security significantly deteriorate.

In sum, one of the reasons why some counterterrorism measures that trade privacy for security might appear to be reasonable is that the majority's security is being purchased at the expense of the minority. However it is possible that a decision to abandon otherwise effective counterterrorism measures that disproportionately endanger a minority might expose other disadvantaged communities to greater actual risk of harm from terrorism. This does not necessarily mean it is acceptable to obtain security at the expense of a minority. Alternative measures or safeguards may be available to ensure that the minority is not sacrificed for the perceived security of the majority. The point here is that the majority is unlikely to perceive the costs that are borne by a minority, or, if they do perceive them, may not be sufficiently concerned with the costs visited upon people other than themselves.

---

42. See Andrew Szasz and Michael Meuser, "Environmental Inequalities: Literature Review and Proposals for New Directions in Research and Theory," *Current Sociology* 45, no. 3 (1997): 99; M.R. Elliott et al., "Environmental Justice: Frequency and Severity of US Chemical Industry Accidents and the Socioeconomic Status of Surrounding Communities," *Journal of Epidemiology and Community Health* 58 (2004): 24.

43. Kristin E. Henkel, John F. Dovidio and Samuel L Gaertner, "Institutional Discrimination, Individual Racism and Hurricane Katrina," *Analyses of Social Issues and Public Policy* 6, no. 1 (2006): 99 at 105–108.

44. Michael Welch, *Scapegoats of September 11th: Hate Crimes & State Crimes in the War on Terror* (Piscataway, NJ: Rutgers Univ. Press, 2006) at 66; Debra L. Oswald, "Understanding Anti-Arab Reactions Post-9/11: The Role of Threats, Social Categories and Personal Ideologies," *Journal of Applied Social Psychology* 35, no. 9, (2005): 1775 at 1776; American Arab Anti-Discrimination Committee, "ADC Fact Sheet: The Condition of Arab Americans Post 9/11" (20 November 2001), http://adc.org/terror_attack/9-11aftermath.pdf; BBC News, "11 September revenge killer guilty," 3 April 2002, http://news.bbc.coc.uk/1/hi/world/americas/1909683.stm.

E. A Social Psychological Need for a Reaction

In times of perceived breakdown in order and security, the social and psychological pressures to react in some way are very powerful. Jeremy Waldron suggests that this psychological reaction largely explains the willingness to trade liberty for an apparently security-enhancing measure.[45] When attacked, people want their government to inflict reprisals and they are less interested in their effectiveness than that "something striking and unusual is being done."[46]

There is also a tendency for a society to display increased solidarity and patriotism following an external attack. The so-called "rally effect" refers to the sudden and substantial increase in public trust in and approval for political leaders after a dramatic international event.[47] The September 11 rally effect was the largest of all recorded rally effects in the United States, producing the highest ever recorded approval rating for any U.S. president, and it lasted longer than any other recorded rally effect.[48]

The surge of patriotism and the desire for social unity may contribute to the willingness with which people sacrifice individual liberties for a perceived collective security improvement.

F. Courts and the Security Versus Privacy Trade-off

It is likely that judicial deference to government also accounts for the extent to which governments are able to curtail liberties including privacy in the name of national security. In recent years, there has been great debate over the institutional competence of judges to deal with questions of national security. Some argue that the courts are not institutionally competent to assess security measures, [49] while others argue that the courts routinely balance competing interests in a wide range of complicated policy domains and that the review of security policies should not be an exception.[50]

Whether or not judges are institutionally competent to consider national security measures, there may be deeper psychological factors at work in the

---

45. Waldron, "Security and Liberty," 209 (n. 2).

46. *Ibid.*

47. Marc J. Hetherington and Michal Nelson "Anatomy of the Rally Effect: George W. Bush and the War on Terrorism" (2003) 36 *Political Science and Politics* 36 (2003): 37 at 37 citing John Mueller, *War, Presidents and Public Opinion* (New York: Wiley, 1973); Richard C. Eichenberg, Richard J. Stoll, and Matthew Lebo "War President: The Approval Ratings of George W. Bush," *Journal of Conflict Resolution* 50, no. 6 (2006): 783.

48. Hetherington and Nelson, "Anatomy of the Rally Effect," 37 (n. 47).

49. Posner, *Not a Suicide Pact*, 35–36, (n. 2); Posner and Vermeule *Terror in the Balance* (n. 2).

50. Daniel J. Solove, "Data Mining and the Security-Liberty Debate" forthcoming *University of Chicago Law Review* 74 (2007–2008) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030.

judicial reluctance to scrutinize them. In particular, judges may realize that, whether or not an impugned security measure would have been effective, they will be blamed should an attack occur after they have ruled it unconstitutional. If the measure is implemented and no attack occurs, those who object to the measure will find it difficult to criticize the government or the courts as it will be hard to show the measure had absolutely no benefit. If the measure is implemented and an attack occurs, the government may be criticized for ineffective security measures, but the courts will not be viewed as responsible. As a result, the obvious and attractive option for the judge who fears the weight of responsibility for national security is to defer to government expertise.

III. REFRAMING THE TRADE-OFF: SECURITY VERSUS SECURITY

Given that the security versus privacy trade-off appears to be biased in favor of security, particularly in times of public insecurity, there is reason to fear that we may too easily sacrifice rights and freedoms such as privacy. Perhaps the bias in favor of security may be resisted by examining how privacy-reducing counterterrorism measures themselves reduce security. In this way, the trade-off analysis may be reframed as one between values that are more commensurable.

Measures and programs intended to increase national security may actually reduce security in certain ways or for certain people. First, security measures may be "security theatre" in that they are reassuring rather than effective in improving actual security. As will be discussed below, this may still be worthwhile to the extent that fear itself produces other forms of harm. However, ineffective security measures may also lull people into a false sense of security, or pose opportunity costs, draining resources away from other public objectives that might improve security. Second, whether effective or not, security measures may create new vulnerabilities. Third, security measures may reduce the security of a minority of the population with unfair and counterproductive results. In the case of counterterrorism measures, the security of the Muslim and Arab population, whose willingness to assist intelligence and law enforcement could be helpful for national security, may be undermined.

A. Security Theatre

The term "security theatre" refers to the adoption of useless or nearly useless security measures in order to provide the reassuring appearance of a response to perceived risks.[51] However, security theatre is not necessarily useless or irrational when the harmful consequences of public fear are taken into account.

The losses associated with terrorism can be divided into two categories. First, a terrorist attack takes a direct toll in lives, damage to property, disruption of

51. Schneier, *Beyond Fear*, (n. 2).

normal life, and immediate remediation efforts. Second, there are several types of indirect harm that arise because of the effect of the attack on the minds of the members of a society. These indirect losses flow from the fear created by the initial attack and may produce a level of casualties comparable to the initial attack. It appears that for approximately one year after September 11 in the United States, there was a reduction in air travel, an increase in highway travel, and a concomitant increase in highway traffic fatalities.[52] Gigerenzer estimates that an extra 1,595 people died on the highways trying to avoid the risk of flying during the year after September 11.[53] He notes that this number is six times greater than the total number of airplane passengers who perished on September 11.[54]

Another type of indirect cost of a terrorist attack is the subsequent expense of security measures that are adopted out of fear of a future attack, such as an elaborate airline passenger screening system. These measures may save lives if they improve actual security or only the perception of security, for the reasons mentioned above. However, where these measures are not effective in achieving either, or the benefits could be achieved more efficiently, the measures impose additional opportunity costs. The resources dissipated on poor security measures should also be understood as the loss of the extra social benefits that the resources could have achieved in terms of life and well-being, for example in health care or education.

Given all of the indirect harms that are suffered as a result of the fearful reaction to a terrorist attack, measures that merely address subjective feelings of insecurity rather than improving real security may be justifiable.[55] Great care should be taken here since this is manipulative of the public, and may reduce trust in the government. Second, it may cause the public to be careless, when vigilance and precaution would be helpful to reduce actual insecurity.[56] Third, governmental attempts to visibly increase security may not be reassuring. This seems to be the case with the color-coded threat warnings in use in the United States, which create a continuous and vague sense of alarm without communicating information of any particular use.

B. Security Measures May Introduce New Vulnerabilities

In order to maintain access to private communications and stored data for surveillance purposes, governments have sought to ensure that "backdoors" or

52. Gigerenzer, "Out of the Frying Pan," 347 (n. 31).

53. *Ibid.*, 350.

54. *Ibid.*; Michael Sivak and Michael J. Flannagan "Consequences for Road Traffic Fatalities of the Reduction in Flying Following September 11, 2001," *Transportation Research Part F* (2004): 301–305.

55. See Cass Sunstein, "Terrorism and probability neglect," *Journal of Risk and Uncertainty* 26 (2003): 121.

56. George Avery, "Bioterrorism, Fear, and Public Health Reform: Matching a Policy Solution to the Wrong Window," *Public Administration Review* 64, no. 3 (2004): 275.

"access points" are built into telecommunications equipment and software. While this has obvious appeal from a government perspective, this approach deliberately introduces vulnerabilities into technologies that are widely used by the public. In addition to the risk of government abuse, the public is exposed to the additional risk that a third party will figure out how to exploit the vulnerability.

This risk is vividly illustrated by the 2006 scandal over the wiretapping of the Greek government by unknown parties. The lawful interception capability built into mobile phones was hacked by unknown parties to intercept the communications of the Greek Prime Minister and other top officials.[57]

The problem of backdoors is also present in software. Backdoors are methods of gaining access to a computer by avoiding the normal authentication requirements. They are sometimes built into software to solve software design problems.[58] However, once present there is a risk that those who introduced the backdoors may misuse them. Furthermore, there is a risk that third parties may discover and use the vulnerabilities.

Although it is difficult to separate fact and legend with respect to government involvement with software backdoors, there is suspicion that some software vendors have placed backdoors into their software at the request of the government.[59] In 2001, a public outcry followed news reports about an FBI project named "Magic Lantern," said to involve a government spyware program circulated by e-mail attachment. The reports indicated that antivirus software companies had worked with the FBI to ensure that their antivirus programs would not detect the spyware.[60] In 2006, the BBC reported that Microsoft was in discussions with the British government to enable it to decrypt the BitLocker system available in some versions of the new Vista operating system.[61] Microsoft's response to inquiries about this was initially evasive, but the company eventually issued a denial.[62]

Apart from the risks of abuse by government, it is clear that the deliberate and general introduction of security vulnerabilities in information and communications technologies creates the additional security risk of outsider attack. The risks associated with vulnerable information and communications technologies are not limited to identity theft, the loss of privacy, or the loss of valuable

57. G. Danezis (trans.) "The Greek Illegal Wiretapping Scandal: Some Translations and Resources," translating the Greek Government Press Briefing 06-02-02, available at http://homes.esat.kuleuven.be/~gdanezis/intercept.html.

58. Kevin Poulsen, "Interbase back door exposed," *SecurityFocus.com,* 11 January 2001, http://www.securityfocus.com/news/136.

59. Declan McCullagh, "'Lantern' backdoor flap rages," *Wired News.com,* 27 November 2001, http://www.wired.com/politics/law/news/2001/11/48648.

60. *Ibid.*

61. Ollie Stone-Lee, "UK holds Microsoft security talks," *BBC News.com,* 16 February 2006, http://news.bbc.co.uk/2/hi/uk_news/politics/4713018.stm.

62. Nate Anderson, "Secret back doors? Microsoft says no, China says maybe," *Ars Technica,* 6 March 2006, http://arstechnica.com/news.ars/post/20060306-6319.html.

business information. The physical security of human rights workers and journalists operating in hostile political environments can be seriously compromised if their activities are exposed.[63]

C. Security Measures May Reduce the Security of a Minority of the Population

After the September 11 attacks, increased attention was devoted to dataveillance for national security purposes. As noted earlier, dataveillance, or the systematic acquisition and integration of multiple streams of data about things and people, poses the risk that incorrect or unreliable data may be used to make decisions about people. In the context of data mining for counterterrorist purposes, the consequences of being flagged as suspicious can be serious.

Technologies for data aggregation and data mining (the automated analysis of large datasets to extract useful information) have led to increased efficiency in gathering and using data.[64] In the context of counterterrorism, the objective is to examine a wide range of data (relating to people, places, things, activities, associations, etc.) in order to identify patterns that point to terrorist activity, and to use those patterns to identify targets for further investigation.[65]

The U.S. Government's "Total Information Awareness" system (later renamed the "Terrorism Information Awareness" system) was intended to link together separate government databases into a virtually centralized database that would permit effective data mining.[66] The eventual inclusion of data from private commercial databases was also contemplated.[67] The U.S. Congress eventually refused funding for the program amid concerns over privacy.[68] Although the Terrorism Information Awareness program has been shut down, data mining projects are continuing elsewhere within the U.S. government.[69]

Counterterrorist data mining projects have been criticized on three fronts. First, they are said to be ineffective due to the necessarily high rate of false positives.[70] Second, they are likely to impose disproportionate burdens on ethnic

63. Affidavit of Patrick Ball in *ACLU v. Miller,* 96-CV-2475-MHS (N.D. Ga.), 24 January 1997, available at http://www.aclu.org/privacy/speech/15525lgl20031009.html.

64. Taipale, "Technology, Security and Privacy" (n. 2) at 177.

65. *Ibid.*, 174; Wayne Renke "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy," 43 *Alberta Law Review* 43 (2006): 779.

66. Defence Advanced Research Projects Agency, "Report to Congress Regarding the Terrorism Information Awareness Program," (2003), available at http://www.eff.org/Privacy/TIA/TIA-report.pdf.

67. Ron Wyden et al., "Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America," *Stanford Law & Policy Review* 17 (2006): 331.

68. *Ibid.*

69. Bruce Schneier, "Why Data Mining Won't Stop Terror," Wired.com, 9 March 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357; Renke, "Who Controls the Past," 789 (n. 65).

70. Schneier, *Beyond Fear*, 253 (n. 2).

and religious minorities. Third, centralized databases of personal information offer a more enticing target for outsider attack and insider abuse, and the compromise of a centralized and comprehensive database is likely to do more harm than the compromise of one of many decentralized and limited databases.

Even if the profiling and data mining efforts are highly accurate and subject to a low rate of errors, the volume of data being collected and mined is so large that there are likely to be many errors. Indeed, the U.S. National Security Agency's controversial communications surveillance program is reported to have produced an unmanageable flood of tips virtually all of which were false alerts.[71]

While the harms associated with the misuse of centralized databases of personal information fall on everyone, it is possible that the dangers of data mining will fall disproportionately along racial, ethnic, or religious lines. Data mining programs based on profiles thought to be correlated with terrorism will generate false positives unless the profile is perfectly predictive of terrorism. If the profiles are based partly on race or religion, the risk of false positives is likely to fall disproportionately on people of the profiled groups.

One of the concerns with the aggregation of data from various sources and its use in data mining projects is that information that is reliable for one purpose may come to be used for much more sensitive applications.[72] The case of Maher Arar illustrates this type of danger. In his case, through a lack of care by the Canadian RCMP with respect to the characterization and handling of information that linked him to an al-Qaeda suspect, Arar came to be suspected of being a terrorist himself, leading to his deportation by the United States to Syria where he faced torture.[73]

One contributing element to Arar's terrible experience was lax data handling by the RCMP. Maher Arar came to the attention of the RCMP because of a connection to Abdullah Almalki, who was suspected of involvement with al-Qaeda.[74] In the subsequent inquiry into the case, the Inquiry Commissioner found that it was reasonable for the RCMP to have investigated Arar, but that the RCMP had provided inaccurate and quite prejudicial information about Arar to U.S. agencies.[75] This information was provided in contravention of RCMP policies that required information to be screened for relevance, reliability, and personal

71. Lowell Bergman et al., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times,* 17 January 2006.

72. Marcus Wigan and Roger Clarke, "Social Impacts of Transport Surveillance," *Prometheus* 24, no. 4, (2006): 389 at 400.

73. Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar, "Report of the Events Relating to Maher Arar: Analysis and Recommendations," (2006) available at http://www.ararcommission.ca/eng/AR_English.pdf.

74. *Ibid.*, 18.

75. *Ibid.* at 18, 28.

information before being shared, and that written caveats be attached to the information to control the uses to which it is put.[76]

The case of Maher Arar illustrates the grave dangers that can face those who find themselves flagged for further terrorism investigation. It also illustrates the manner in which information gathered into databases can be used for purposes to which it is unsuited, with results that are catastrophic to the individual. To the extent that data mining projects are based on a terrorist profile that specifies young, Muslim males of Arab ethnic background, and to the extent that data mining creates a large number of false positives, this minority group will find itself more frequently flagged for further groundless investigation. This elevated level of interaction between the suspect group and the security community increases the chances that mistakes will be committed as in the case of Maher Arar.

In this way, national security is pursued in a manner that reduces the security of a minority within the population. Not only does this reduce the security of individual members of the minority group, it may reduce overall national security. This is because the minority group may justifiably come to feel alienated and defensive, as well as fearful of contact with intelligence and law enforcement officials. Their assistance and insight in fighting terrorism might be partly forfeited as a result.[77]

IV. CONCLUSION

In the aftermath of the September 11 attacks, it was widely accepted that it would be necessary to trade some personal privacy in order to obtain improved national security through greater government surveillance. The concept of an inevitable trade-off or balance between the two is longstanding, but tends to emerge with renewed vigor at times of national insecurity. This was certainly the case after September 11, as numerous governments including Canada moved to strengthen their counterterrorism efforts through increased surveillance and to implement various data-gathering and data mining programs. The harms associated with this erosion of privacy were often ignored or those who raised them were denigrated.[78]

For various reasons, the value of security tends to trump that of privacy. Perhaps one way to ensure that the debate is not prematurely ended in this way

76. *Ibid.*, 18.

77. Michael P. O'Connor and Celia M. Rumann, "Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland," *Cardozo Law Review* 24 (2003): 1657 at 1737.

78. Testimony of John Ashcroft. Preserving our freedoms while defending against terrorism. Hearings before the Senate Committee on the Judiciary, 107th Congress, 1st Session, 2001, 316.

is to focus on the ways in which a privacy-reducing measure actually reduces security. In this way, values of similar weight may be considered in the trade-off. Counterterrorism measures may imperil the physical security and lives of individuals by introducing new vulnerabilities or by sacrificing the security of a minority for a *feeling* of security for the majority.

This paper has not sought to answer the difficult question of the justice of specific counterterrorism measures. However, it is clear that the justice of the trade-off is a complex matter. Actual harm may flow from mass panic, so that measures to address the *feeling* of insecurity may be justified. Furthermore, certain types of terrorist attacks may disproportionately harm a minority such that a refusal to employ an effective counterterrorism measure might leave them bearing greater risks.