The Diva and Destiny: Can the Voter Be Appeased With Fatalism?

Michel van Eeten and Frederic Bouder***

Over recent years there has been a growing concern for the tendency of modern Western public administrators and regulators to overregulate risk – also coined the risk-regulation-reflex (RRR). Too often public decision-makers react to instances of risk with knee-jerk interventions such as increased regulation and inspections. The underlying assumption behind this response is that fatalism, in the sense of accepting risk, is no longer tolerated by citizens and has no place in the current political discourse. This paper challenges that assumption and suggests, on the contrary, that political messages about accepting risk deserve a revival. A balanced perspective can help Western society avoid the pitfall of overreacting to risk.

I. Introduction

What can our government do against 'bad events' such as train crashes, food contamination or financial scams? Many experts, administrators and politicians would agree that scientific processes to balance risks, benefits and costs are the best way forward. The assumption is that, as a society, we are better off when we rely on scientific risk assessments. In a nutshell, sound trade-offs between risks, costs and benefits save more lives than the expensive illusion that all 'bads' should be averted at any cost[1]. 'Risk-based' approaches have acquired an almost revered status in European regulatory circles. They are a guiding principle in domains as diverse as chemical regulation, food safety, child protection, finance, education, mental health and housing[2]. Yet, what really happens when something goes wrong? Do politicians stick to science or do they suddenly turn 'risk-averse'? For over twenty years, scholars and decision-makers have cast doubts on whether decision-makers, when in doubt, use much science at all. European case studies have uncovered many examples of precautionary actions that bypass scientific assessments, ranging from bans on hormones in beef, ground nuts or brominated flame retardants, with comparatively little attention paid to issues with less direct impact on health or the environment such as banking or internet transactions[3]. Some have argued that Europeans are behind the Americans with regard to developing a risk-based regulatory culture , and that there has been a transatlantic shift in regulatory stringency towards Europe, which is part-due to unparalleled pressures

* Michel van Eeten is Professor of Public Administration at the Faculty of Technology, Policy and Management at Delft University of Technology, The Netherlands.

** Frederic Bouder is Assistant Professor in the Faculty of Arts and Social Sciences' Department of Technology and Society Studies at Maastricht University, The Netherlands.

1 W. Kip. Viscusi, *.Fatal Tradeoffs: Public and Private Responsibilities for Risk* (Oxford: Oxford University Press 1995); John Graham "Why Governments Need Guidelines for Risk Assessment and Management" in OECD (eds) *Risk and regulatory policy: improving the governance of risk* (Paris: OECD, 2010).

2 Marieke De Goede, "Repoliticising Financial Risk," 33(2) *Economy and Society*, (2004), pp. 197–217; Henri Rothstein, Michael Huber and George Gaskell "A Theory of Risk Colonisation: The spiralling regulatory logics of societal and institutional risk", 35 (1) *Economy and Society* (2006), pp. 91–112; Inspectorate of Education of the Netherlands, *Risk-based inspection as of 2009: Primary and Secondary Education* (The Hague: Inspectorate of Education, 2009); Julia Black "Risk-based regulation: choices, practices and lessons learnt", in OECD (eds) *Risk and regulatory policy: improving the governance of risk* (Paris: OECD, 2010);Ragnar E. Löfstedt Risk versus Hazard – How to Regulate in the 21st Century European, 2 *Journal of Risk Regulation* (2011), pp. 149–168.

3 Jonathan B. Wiener, Michael D. Rogers, James K. Hammitt, J., and P. H. Sand, P. (eds) , *The Reality of Precaution: Comparing Risk Regulation in the United States and Europe*, (Washington DC and London: Resources for the Future, 2010); Ragnar E. Löfstedt "Risk versus Hazard – How to Regulate in the 21st Century European", 2(2) *European Journal of Risk Regulation* (2011), pp. 149–168.

put on European regulators to "do something"[4]. This article explores real-life decisions where regulators are caught between a rock and a hard place. First it briefly addresses the question of why the political debate pushes politicians to take such a hard and automatic stand for risk elimination. Nonetheless, politicians do at times try to justify some form of fatalism to the public, out of conviction or necessity. We look at what can go wrong in such cases, harking back to a message that is often heard in such cases: "Nothing is 100% safe". Finally, we look at how fatalism can be made palatable to the public.

II. Risk and democracy

The obituaries that appeared in newspapers after the recent death of Dutch former minister of the Interior Hans Dijkstal all made reference to his characterization of voters as "pampered divas." Dijkstal's criticism of the electorate earned him a measure of respect among journalists and others, but it was mainly respect of the kind reserved for tragic figures fighting for a righteous but hopeless cause, like a politician who refuses to cater to the sycophant practice which we call democracy.

One newspaper ran an anecdote in which Dijkstal is at a fair for senior citizens. A visitor asks Dijkstal what his political party (the VVD) wants to do for the elderly. "If possible, nothing," Dijkstal answered. The woman was speechless, wrote the reporter. Some of the woman's amazement may have been a projection of the journalist's own disbelief.

At another point Dijkstal said, "Democracy is not a jukebox with everyone's favorite song." One of the "favorite songs" that he so detested was society's tendency to view government as responsible for every conceivable risk. We cannot blame government for every problem, Dijkstal said. In essence, his message was a call for some degree of fatalistic acceptance. Society has to accept that problems are sometimes unavoidable. Few politicians have taken up this call, although none can deny its veracity. In the heat of the political debate after any calamity the fear of a backlash from the media and voters prevents politicians from stating the obvious: Problems are just a part of life. In other words, the once prevalent notion of fatalism is considered to be an outdated concept for modern society and political discourse seems to treat it as a taboo. Dijkstal's electoral decline also seems to confirm, for those seeking confirmation, the power of this taboo.

The very notion of risk can be seen as a promethean emancipation from the 'Gods', when people broke loose from the constraints of the past and subjected long-held beliefs about fatalism to open challenge[5]. Yet, today's taboo on fatalism is also part of a larger phenomenon, namely, government that exhausts itself in a compulsive endeavour to avoid risk. Playing its opposite is a small army of experts adept at explaining why such government is undesirable. These authorities' main critique is, in short, that trying to eliminate risk is counterproductive. New rules do not increase our actual safety; in some cases they may even make us less safe because when we become obsessed by the negatives we tend to overlook benefits and neglect risk/risk trade-offs[6]. For example, the time-consuming security checks at airports are responsible for thousands of extra traffic deaths each year – in part because it prompts people to travel by car instead of by plane[7]. In just the first three months after 9/11/2001 this led to some thousand extra road fatalities in the U.S. alone.[8] Efforts to eliminate risk do not always make us safer, and on top of that they may saddle society with disproportionally high costs and infringements of our freedom.[9]

The experts see their diagnosis confirmed in government responses to every new safety incident. Their commentary has by now become part of the ritual. Every calamity becomes the subject of numerous editorials in which the experts explain why the

4 Ragnar Löfstedt and David Vogel, "The changing character of regulation: a comparison between Europe and the United States", 21(3) *Risk Analysis* 21, (2001), pp. 399–405; Giandomenico Majone, "Regulatory Legitimacy in the United States and the European Union", in: Kalypso Nicolaidis and Robert Howse (eds), *The Federal Vision*, pp. 252–274 (Oxford: Oxford University Press, 2001); David Vogel, *The Politics of Precaution. Regulating Health, Safety, and Environmental Risks in Europe and the United States* (Princeton and Oxford: Princeton University Press, 2012).

5 Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, 1998).

6 John D. Graham and Jonathan B. Wiener (eds.) *Risk versus Risk: Tradeoffs in Protecting Health and the Environment* (Cambridge, MA: Harvard University Press, 1995).

7 Garrick Blalock, Vrinda Kadiyali en Daniel H. Simon (2009), "Driving fatalities after 9/11: a hidden cost of terrorism", *Applied Economics*, 41 (14), pp. 1717–1729.

8 Michael Sivak, Michael J. Flannagan, "Consequences for road traffic fatalities of the reduction in flying following September 11, 2001", *Transportation Research Part F* 7 (2004), pp. 301–305.

9 Aaron Wildavsky provides an authoritative analysis of this problem in *Searching For Safety* (New Brunswick, NJ: Transaction Books, 1988). This point has been brought up by numerous authors in the past decade. See for example: Frank Furedi, *Culture of Fear*, (London: Continuum, 2002). See also his essay: "Precautionary culture and the rise of probabilistic risk assessment", *Erasmus Law Review*, September 4, 2009.

closure of airspace was overblown, why the oil spill is not as bad as intimated, and who has what to gain by exaggerating the dangers of a flu epidemic.[10]

Their diagnosis can count on widespread support. As to the proper treatment for this compulsive pattern of behaviour, the experts are less outspoken. Frank Furedi calls for "rational trade-offs."[11] Margot Trappenburg insists on "an unhurried well-considered approach".[12] Many of these proposals, however, focus attention on the wrong cause, or rather, at the wrong level of analysis. They unfairly blame an institutional problem on failings at the level of the individuals who operate within those institutions. Just as anyone else, politicians and public officials are undoubtedly afflicted with cognitive handicaps that cripple their attempts to evaluate risk[13]. But even if they could make better use of risk science, they would still be locked in a political establishment that forces them to ignore the outcomes of these assessments. After a calamity, or when a potentially dire risk suddenly emerges, it is tough to convince voters that they ought to just accept the risk. Politicians operate – not entirely without reason – under the assumption that the electorate and media find such fatalism wholly unacceptable.

The compulsive pattern of risk aversion is upheld by the rules of political debate, not by the views of politicians and public administrators. The people responsible for public policy have no repertoire at hand to make risk acceptance attractive to voters. 'Tolerability of Risk' models may be efficient to guide managerial decisions, they will fail to appease public opinion when trains crash and factories blow up[14]. In other words, if we want to break the pattern we have to ask the question: Is there a way to appease voters with fatalism?

III. Rules of the debate

Risk is the probability of loss. While "probability" is difficult to visualize, "loss" is easy to imagine. And to fear. Loss is known to dominate our perception of the risk[15]. And to make things more complicated, risk related loss is not always linked to a clear prospect of risk related benefit. In the real world of business and government decisions, risk imposers routinely ask others to bear the risks on their behalf. So "loss" tends to dominate the debate. As a consequence, loss is generally approached using a simple moral scheme: "Wherever there is a threat of loss, something has to be done." Most political positions follow this scheme. We call it "commitment" or "engagement."

For elected representatives, preventing "loss" is tantamount to political capital. You can use it to produce opportune positions. It also buys media attention. If the loss appears pale in the harsh lights of the cameras, then simply apply a bit of rouge. It's for a good cause. Dutch parliamentarians concede that they go about their days in a constant state of "astonishment," "shock" and "unpleasant surprise."[16]

Loss can be depicted in a variety of ways. One of the most popular is the tale of impending doom.[17] Politics is dominated by these stories, expressing what German philosopher Rüdiger Safranski calls the "public ethic of disaster avoidance."[18] Disaster comes in many forms – climate change, Islamization, declining language proficiency of text-messaging youths, disease spread by public swim-

10 See for example Luc Verhey, "Openbaar bestuur verkrampt door as" ["Government cramped by ash"], *NRC Handelsblad*, 20 April 2010.; Kees Camphuysen, "Ramp in Golf van Mexico wordt overdreven" ["Disaster in Gulf of Mexico exaggerated"], *NRC Handelsblad*, 10 May 2010.; Simon Jenkins, "Volcanic ash is the new swine flu panic", *The Guardian*, 19 April 2010.

11 Frank Furedi, "Precautionary culture and the rise of probabilistic risk assessment", *Erasmus Law Review*, September 4, 2009.

12 Margot Trappenburg, "Waarom het allemaal niet lukt", in Jan van Tol, Ira Helsloot, Ferdinand Mertens (eds) *Veiligheid boven alles? Essays over oorzaken en gevolgen van de risico-regelreflex*. (Den Haag: Boom , 2011), pp. 35–50

13 About forty years ago economists and psychologists started to systematically uncover the cognitive factors that affect risk perceptions. The take home lesson of this major endeavour is that human rationality is much more complex than what conventional views on rational decision making would suggest. See among seminal papers Amos Tversky and Daniel Kahneman, "Judgement under Uncertainty. Heuristics and Biases", 85 *Science* (1974)pp. 1124–1131; Baruch Fischhoff, Paul Slovic and Sarah Lichtenstein "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits", 9 *Policy Science* (1978), pp. 127–152; Paul Slovic, "Perception of Risk", 236 Science(1987), pp. 280–285.

14 On the origins, pros and cons of risk tolerability models see Frederic Bouder, David Slavin and Ragnar Löfstedt (Eds) *The Tolerability of Risk: a New Framework for Risk Management*, (London and Sterling (VA): Earthscan, 2007).

15 For an illuminating discussion on the subject see Chapter 28 of Daniel Kahneman, *Thinking fast and slow*, (London and New York: Penguin Books, 2011).

16 J. Th. J. van den Berg, "De parlementaire orde is een politieke orde" ["Parliamentary order is a political order"], in: Tweede Kamer der Staten-Generaal, *Vertrouwen en zelfvertrouwen: Analyse en aanbevelingen. Parlementaire zelfreflectie [Confidence and self-confidence: Analysis and recommendations. Legislative self-reflections]*, (The Hague, 2009) pp. 152.

17 See the discussion on "stories of decline" in Deborah Stone, *Policy Paradox: The Art of Political Decision Making (third edition), (*New York: W. W. Norton & Company, 2001).

18 Rüdiger Safranski, *How much globalization can we bear?* (Cambridge: Polity Press, 2005).

ming water, a thirteen-year-old schoolgirl's plan to take a solo sailing journey. But whatever tale is told, the ending is always the same: Something has to be done.

Politicians have little to gain from departing from this moral scheme. The only other way out is to keep quiet about the risk. But that can be tricky. Keeping quiet gives political rivals a chance to take up the cause and present themselves as its champion. After all, the true champion is the one who is most shocked and intervenes most decisively. Engagement is therefore inextricably linked with the interventionist state, which increasingly penetrates into the lives of its citizens under the guise of eliminating risks and their terrible consequences.[19]

Whether we are really better off pursuing a certain intervention is of secondary importance. It is always better to do something than to do nothing. That is a categorical moral position, not a consequentialist one. For politicians, this is a convenient approach. Intervening is intrinsically good, so little evidence is needed to demonstrate that an intervention is desirable. Action is always better than inaction. Anyone who disputes that is morally suspect and quickly disqualified as a cynic. There are countless examples from everyday government practice. When administrators at the European Medicines Agency were told that very small quantities of a carcinogen impurity had contaminated an HIV drug, they did not think twice. They suspended the product, even though the risk was very small. Similarly, health authorities in Spain stopped a batch of the anti-HPV vaccine Gardasil after two girls overreacted. The fact that their severe agitation was most probably of a psychological nature did not change anything[20].

Arguments suggesting that society would be better off accepting the occasional misfortune are perceived as abstract. They are easily eclipsed by the sheer dramatic power with which human and material loss is brought into view. Anyone who opposes the introduction of a nationwide database with records on all Dutch children has to explain why they accept leaving children exposed to the dangers of abuse and even death. An example, like the 2004 abuse and death of three-year-old Savanna, is readily found. The fact that there is little evidence to support the claim that such a database prevents a tragedy like that of Savanna doesn't matter to its advocates. For many voters, it is more reassuring to ally themselves with the idea that they at least tried to do something, rather than align themselves with the skeptics.

The fact that every misfortune can be presented as avoidable merely strengthens this mechanism. In the Netherlands, the Dutch Safety Board has investigates hundreds of accidents and disasters. Only in a handful of cases, the Board concluded, "These things happen, no one failed." In the wondrous universe of the Safety Board, virtually all accidents are avoidable. Politicians are forced to operate in that world too.

We are seduced to interpret threats and risks as caused by someone else's negligence.[21] As if misfortune is an intruder that can gain entry only because someone forgot to double lock the door. Politics is the identification of who it was who forgot to lock the door.

IV. Fatalism at someone else's expense

When it comes to eliminating risk, government sometimes has no choice but to admit its powerlessness. An example is when harm has already been done and the only thing left is to explain why it was not prevented. That brings us to the second question: What goes wrong when administrators try to sell fatalism to the public?

The safety risks associated with new technologies are considerably less dramatic than child abuse and plane crashes. Strict government-set safety regulations ensure this. Techniques such as cost/benefit analysis, risk/benefit analysis and the like are worthwhile rationalizing tools that mediate this effort. Yet even the modest risks that do remain tend to be amplified and acquire a life of their own. They arouse emotional appeals and sometimes large-scale resistance from within society. From the underground storage of CO_2 to UMTS antennas, 'smart' electricity meters and car-installed devices for road pricing schemes: new technologies everywhere are met with distrust.

19 See for example Paul Frissen, *Gevaar verplicht: Over de noodzaak van aristocratische politiek [Danger required: On the need for aristocratic politics]* (Amsterdam: Gennep B.V., 2009).

20 European Medicines Agency (EMA) *Benefit/risk communication by the European Medicines Agency: a study of influential stakeholders" expectations and attitudes*. (London: EMA, 2011).

21 Marjolijn Drenth von Februar cites political philosopher Susan Mendus, who argued that modern liberal political theory is dominated by a desire to liberate the world from random forces. See Marjolijn Drenth von Februar, "De voors en tegens van het lot" ["The pros and cons of fate"], in Hans Boutellier (ed.), *Leven in de risicosamenleving [Life in the risk society]* (Amsterdam: Amsterdam University Press, 2005), pp. 19–26.

When confronted with some compromise of safety, public administrators and technology operators often hark back to a fatalistic mantra: "Nothing is 100% safe." That message is as unacceptable as it is true. Why? Let's look at an example: the introduction of a Dutch public transit smartcard .

1. Smartcard ticketing for public transportation

On January 2, 2008, it became known that two German hackers had cracked the security algorithm of the chip on the Dutch public transit smartcard. TransLink Systems (TLS), a joint venture company that produces the cards for the public transit carriers, played the incident down:

> "Just because one card was cracked... doesn't mean that all cards have been cracked. The public transit smartcard is still safe to use. But we all know that any type of security will be cracked sooner or later.... No system can be 100% secure."[22]

TLS claimed that it would take weeks and thousands of euros worth of equipment to crack just a single card. To make a long story short, a few weeks later a computer science student cracked a card with his laptop in under a minute. In the months that followed TLS was the subject of intense public criticism. After all, the hackers had bypassed the card's security mechanisms much more easily than the company had predicted. TLS's credibility was in tatters. Political pressure eventually rose to the point that the state secretary stepped in. She pledged to accelerate the switch to another chip that, though more costly, was also more secure. The project was delayed and faced huge budget overruns.

Dutch debate on the cracked public transit smartcard closely resembles that on hacked ATM cards. Why do security risks of such modest proportions provoke so much commotion? Are public administrators right after all to characterize citizens as spoiled divas incapable of tolerating even the most inconsequential of risks?

Several things were wrong with the fatalistic message articulated by TLS, and in its wake, by the state secretary . To calm the unrest, they played down the risk. Inadvertently, this made any new information about the perceived threat newsworthy. Every piece of information that followed further undermined TLS's claim that no serious threat existed. So it lost authority. The suspicion raised was that the actual risk was much greater than anyone was willing to admit.

But the message had another even more devastating effect: the desire to downplay the risk in fact implied that the magnitude of the risk is the essence of the issue. This may seem obvious, but it's not. The reason why the actual magnitude of the risk mattered, is because it was borne by others than TLS. So by downplaying the risk, TLS inadvertently signalled that they were not the ones burdened with the consequences. The exact size of the risk matters only to the one threatened by it. The more emphatically TLS downplayed the risk, the stronger the message became, "The risk is yours, not ours."

This brings us to the heart of the issue: The powerlessness that TLS admits by reiterating the mantra "nothing is 100% secure" is more than mere honesty. It is actually an attempt to shift responsibility. Implicitly, TLS said: "I'll do my best to protect you. Beyond that, you'll just have to learn to live with it." This message can be summarized as *fatalism at someone else's expense.*

It is not the fatalism of this message that is wrong, but rather the allocation of the consequences of that fatalism. In essence, the dilemma is this: by what principle should we proceed when we are faced with such powerless? In many such cases, the powerlessness to prevent a certain risk could be made acceptable simply by compensating the losses to others. The question of the exact size of the risk then becomes irrelevant, at least as a matter of public debate.

After the first attempts at cracking the public transit smartcard, TLS could have responded with a different message, such as:

> "Every technology can be cracked. The public transit smartcard will also be cracked sooner or later. TLS offers all of its customers a guarantee: We will immediately reimburse any direct losses they experience due to a cracked card. Still, we consider the chance of fraud to be minimal. The card is not an attractive target for criminals. In London a similar public transit smartcard has been in use for years without major cases of fraud."

TLS's responses did contain elements of this message. But they were completely overshadowed by the

22 TransLink Systems, press release January 15, 2008.

company's efforts to convince the public that the card was still secure. As early as January 2008, TLS announced in the margins of a press release that if passengers did incur losses due to the hacked security, all direct financial damages would be reimbursed. The idea was that this would be included in the general terms of use of the smartcard. But that is unlikely. The terms are ambiguous about this at best. But that aside. More important is that TLS completely overshadows this statement with attempts to downplay the risk, both qualitatively and quantitatively. On January 15, the company issued no less than four press releases, the last of which was a summary of the previous three. Only the first release contains, all the way at the end, a short remark about compensation for financial damages – just 60 of the some 3000 words with which it attempted to calm the uproar that day. Once again, by addressing the technical risks at such lengths TLS is implicitly saying that the risks are important to all of us and that decisions on the public transit smartcard must take this into consideration.

V. The economic value of fatalism

1. Internet banking

The case of the public transit smartcard is tragic, because the organizations involved suffered substantial damage from the uproar, yet there was never any real threat to the public. The case of Internet banking is different. Here, consumers regularly suffer significant losses due to fraud. For years, Internet banking has been attacked successfully and on a large scale by criminals. Strangely enough, this security threat has raised little commotion in political circles.

The ritual followed is the same as that of the public transit smartcard. The banks conceal security infringements if at all possible. When forced to respond they downplay incidents, then point to their efforts to increase security, again sealed with the fatalistic mantra: "it is impossible to guarantee 100% security."

Is this another case of fatalism at someone else's expense? Banks routinely say that they reimburse damages. In this respect, they are ahead of TLS in understanding how fatalism can be made palatable to the public.

But their message is not consistent, and there are no formal guarantees for customers.

Banks communicate ambiguously about who is liable for losses. This seems partly deliberate. Obviously they want to preserve public confidence in the electronic payments system. But banks also want their customers to bear some part of the responsibility, to prevent sloppiness. Regulations in this area permit this, partly because they are always a step behind fraud, which is complex and continually changing.[23] In practice, the banks are the ones that decide whether a customer's losses will be reimbursed. Legal action against such decisions is difficult. The costs of a court case are high. Plaintiffs can be held liable for all legal costs if they lose, and judges tend to view the banks' technical claims with an uncritical eye.[24]

The banks' claim that they reimburse losses is not monitored by any external party.

Damage compensation does reach some customers, but not all fraud victims are so lucky. In December 2008, the consumer television program 'Kassa' pleaded the case of 18 customers of the Dutch PostBank who had been robbed of €212,000 in total due to debit card fraud. The bank had denied all of their claims. The publicity triggered by the program prompted the bank to pay the damages after all. In fact, there were some 200 victims, not 18. All from a single attack on one bank.

The Dutch Banking Association (NVB) did no better in its response to the crack of the EMV chip on debit cards. Here too the focus was on downplaying the risk – a tactic that not only arouses distrust, but again inadvertently emphasizes the need for the public and political leaders to understand the size of the risk. Nowhere is the customer mentioned. Here again the NVB could simply have formulated an acceptable fatalistic message: "Every technology can be cracked. This is true for the EMV chip as well. We will compensate any and all losses to custom-

23 See for example Reinhard Steennot, "Allocation of liability in case of fraudulent use of an electronic payment instrument: The new directive on payment services in the internal market", 24 *Computer Law and Security Report (2008), pp. 555–561.; Gerald Spindler, "Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären: Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler", 2007*. Available on the internet at <http://www.bsi.de/literat/studien/recht/Gutachten.pdf>. (last accessed on 16 July 2012)

24 Steven J. Murdoch, "Reliability of chip & PIN evidence in banking disputes", 6 *Digital Evidence and Electronic Signature Law Review* (2009), pp. 98–115. Available on the Internet at <http://www.cl.cam.ac.uk/~sjm217/papers/deaeslr09reliability.pdf> (last accessed on 16 July 2012).

ers as a result of fraud due to cracked debit cards. We do that now and we will continue to do so in the future. At the same time we will obviously continue to ensure that such losses are minimal. That is in everyone's interest. The switch to the EMV chip is a step in that direction." By not responding in this way, they unintentionally ensured that every new assault on the technology was newsworthy. It's interesting to note what NVB spokesman Michel Noordermeer actually did say: "Whatever method is conceived, at some point criminals will find holes in the system. Unfortunately, nothing can be 100 % secure. The aim of the campaign '3x Okay' is to inform customers of their responsibility and to raise awareness of the potential threats. By following the instructions from the campaign, consumers can ensure that their electronic transactions are safe and that the chance of problems is practically zero. If money is still stolen despite these precautions, the bank provides compensation, just like they do in cases of debit card fraud.'[25]

2. Other risks of electronic banking transactions

This incident does not stand on its own. Banks regularly deny other valid claims. In the first years in which 'skimming' took place, the banks routinely rejected damages claims. They checked whether a disputed transaction had been authenticated by the customer's personal identification number. If the PIN was entered they concluded that the customer had made the transaction or had failed to keep the PIN private. Judges tended to follow them in this reasoning. Mistakenly, it turns out, because criminals had developed methods to discover the PINs for the cards they copied. Banks began to refund the losses only after skimming was taking place at such a large scale that it could no longer be denied. At this point the banks also began to trace victims themselves. In the meantime, a large group of customers had already become victims through no fault of their own. The size of this group is unknown. In the 1990s several thousand British victims began a lawsuit against 13 banks which had denied their claims. The banks won the case.[26]

This suggests that substantial losses are being borne by customers. Although banks in the Netherlands do not publish statistics on Internet banking fraud, their British colleagues do. In 2008, the UK registered some €360 million in "card not present" fraud, the bulk of which is online payments fraud. For the sake of comparison, losses from skimming in the UK were €190 million over the same period.[27] Dutch banks did recently begin to publish, at government's request, figures on losses from skimming. In 2008 these totaled € 31 million.[28] If the proportion between skimming and Internet fraud in the Netherlands is the same as that in the UK, fraud in the Netherlands would add up to some € 59 million. The real losses may be less, but the comparison gives some indication of the amounts involved. Some of these losses are borne by customers. A recent UK survey found that 20 % of customers who suffered losses were not compensated by their bank.[29]

To summarize: the banks, and beyond them, the political establishment, have a fatalistic message which they could make palatable to the public. But when the actions of those in charge speak differently than their words, their message and their credibility are undermined.

Reputational damage is not the only thing at stake here. If misgivings among consumers lead to slower growth in the use of the electronic payment system, this damaging effect would be many times larger. Migration from offline to online transactions has led to enormous savings. Branch offices can be closed, fewer employees are needed, and expensive paper processing can be scaled down. Every delay in that migration is equivalent to a loss of efficiency that far outweighs the magnitude of the fraud.

25 Gijsbert Bouw, "Internetbankieren is niet veilig", Reformatorisch Dagblad, 2 February 2008, available on the Internet at <http://www.cs.ru.nl/B.Jacobs/PRESS/reformatorisch-dagblad-internetbankieren-02–01–08.txt> (last accessed on 16 July 2012).

26 Ross Anderson, Mike Bond and Steven J. Murdoch, "Chip and Spin", 22 March 2006, available on the Internet at <http://www.cl.cam.ac.uk/users/sjm217/papers/cl05chipandspin.pdf> (last accessed on 16 July 2012).

27 APACS, *Fraud: The facts 2009. The definitive overview of payment industry fraud and measures to prevent it*, London, 2009. Available on the Internet at <www.theukcardsassociation.org.uk/files/fraud_the_facts_2009.pdf> (last accessed on 16 July 2012).

28 "Schade door skimmen 31 miljoen" ["Losses due to skimming 31 million"], *NRC Handelsblad*, 18 May 2009, available on the Internet at <http://www.nrc.nl/economie/article2244994.ece/Schade_door_skimmen_31_miljoen> (last accessed on 16 July 2012).

29 Which?, "Fraud victims struggle to get money back", date ? 2009, available on the Internet at <http://www.which.co.uk/news/2009/06/fraud-victims-struggle-to-get-money-back-179150.jsp.> (last accessed on 16 July 2012). See also: Murdoch, "Reliability of chip & PIN evidence in banking disputes", *supra* note 24.

3. Credit cards

Credit card companies understand the economic value of fatalism. Credit cards are much more fraud-prone than debit cards. Yet credit card companies still reimburse all losses experienced by card holders. They are also very reluctant to introduce new security measures that would require the card holder to go through additional verification steps. The reason: more steps means less growth in credit card use. That usage is how these companies earn their profits. Earnings from credit card transactions have for years grown much more rapidly than fraud. Relatively speaking then, fraud is on the decline. It currently fluctuates around 0.05 % to 0.07 % of the total transaction volume. This is about seven cents for every hundred euros charged.[30]

It seems reasonable to ask customers to bear a part of the risk. But the banks are actually better off not sharing the risk with the customer. In the 1970s, the US government passed legislation making banks entirely liable for losses, with just a small waiver for the customer. A VISA director told me that the financial sector initially fought the law tooth and nail. But they quickly realized it was a blessing in disguise. The banks no longer had to justify their investments in security, because they were the ones who would bear any losses. As a result, they spent much less on security than the European banks did.[31] These savings alone outweighed the losses that they had to reimburse. More importantly, customer convenience was not hindered by additional security measures. This was one obstacle less in the migration to an online payment system.

Lack of safety then has definite benefits. This observation is also more broadly true for the Internet as infrastructure. Our computers are easily infected with malicious software because they allow us to run any program that we choose. But that is also precisely why computers have made possible a tidal wave of innovations.[32] Many proposals to increase the security of the Internet sacrifice innovation potential for more control. A fatalistic strategy tolerates the bedlam. In doing so, the door is left open for great economic and social gain.

VI. Selling fatalism?

Intolerance to fatalism saddles us with high costs, in terms of money but also in human lives. As mentioned before, all the new security measures at airports cause thousands of additional road deaths, because the additional travel time pushes more people to the much less safe alternative of road travel.[33] That brings us back to the question of how fatalism can be made palatable to the public.

Most politicians believe that there is no way to make fatalism acceptable to voters. In this respect, Hans Dijkstal's colleagues seem to silently share his sentiment about voters as pampered divas refusing to accept misfortune as a part of life. If that is true, how can we then break the pattern of a government that reacts compulsively and disproportionally to risk?

The assumption that voters never accept fatalistic messages has un underlying element of complacency. It presumes that the message itself is correct, but that voters don't want to face the truth. But is that true? In our examples we saw that the message itself was flawed, that they were covert attempts to shift responsibility. Those cases do not stand alone.

Whether voters accept problems as part of life depends not only on their individual outlook on life, but also on the meaning that is assigned to those problems. In the face of adversity, decision-makers often fall back on the mantra "nothing is 100 % safe." But this, as we saw, is a form of fatalism at someone else's expense. It is resignation to fate but without having to share that fate. It entirely leaves out the one evoking it. In response to unrest among residents of Barendrecht about plans by Shell and the government to store CO_2 in the ground under their homes, provincial administrator Van Heijningen reverted to the mantra: "It's impossible to give a 100 % guarantee that nothing will happen."[34]

We reject this message because implicitly it tells us, "I'll do my best, but something could still happen

30 See for example VISA, *Payment card fraud*, available on the Internet at <http://www.visaeurope.com/pressandmedia/factsheets/paymentcardfraud.jsp> (last accessed on 16 July 2012). See also: Richard J. Sullivan, *The benefits of collecting and reporting payment fraud statistics for the United States,* available on the Internet at <http://www.kansascityfed.org/Publicat/PSR/Briefings/PSR-BriefingOct09.pdf> (last accessed on 16 July 2012).

31 Ross Anderson and Tyler Moore, "The economics of information security", 314 *Science* (2006), pp. 610–613.

32 Jonathan Zittrain, *The Future of the Internet: And How to Stop It*, (New Haven: Yale University Press, 2008).

33 Michael Sivak, Michael J. Flannagan (2004), Consequences for road traffic fatalities of the reduction in flying following September 11, 2001, *F 7 Transportation Research Part* (2004), pp. 301–305.; Garrick Blalock, Vrinda Kadiyali en Daniel H. Simon "Driving fatalities after 9/11: a hidden cost of terrorism", 41 (14) *Applied Economics*, (2009), pp. 1717–1729.

and if it does I cannot be held responsible." In other words, you'll just have to swallow it. That last part is why it is categorically rejected by all – especially when risk is being thrust upon us. But that doesn't mean we are all pampered divas.

1. One for all, all for one

New principles are needed to give a meaning to problems beyond docile resignation to fate, especially a fate in which you bear the risk and someone else reaps the benefits. Such a principle could be "those who profit from a risk must share in bearing it." In the Barendrecht case, that suggests two options to make the risk more palatable. First, the residents should benefit, in as far as possible, from the risk they bear. Second, those who benefit from the project, its initiators, should, in as far as possible, also bear part of the risk. Neither of these options requires regulations to frenetically hold risk in check.

The first option, for residents to share in the benefits, is a proven strategy. Yet it does not seem to have been in play in the Barendrecht case. The local government firmly opposes the project, which suggests that no exchanges of interests took place. Reconstructions of the process suggest that the central government and Shell did not try to reach a package deal with the local authorities.

The second option could be pursued, for example, if Shell or the government had guaranteed full compensation for any and all damages. If the underground storage really is as safe as they say, there is no reason to shy away from such a guarantee. This arrangement would be simplest for property damage. One prediction is that subsidence could occur. So Shell and the national government could take full liability for any damage to property due to subsidence. For health risks it may seem callous to speak in terms of financial liability. But here it is instructive to realize that the airline industry has used this system to good effect. When a plane crashes the airline company is immediately confronted with huge damages claims – claims that threaten the very survival of the company. That is precisely why the companies do everything in their power to prevent accidents. And successfully so.

Health risks can also be shared symbolically. One of us once heard about a DuPont policy requiring the directors of large chemical plants to reside on the grounds of the plant. This is probably an apocryphal tale, but it illustrates an elegant form of sharing the burden of risk. Someone who braves a risk with his or her family is much more credible than someone citing from a pile of bought-and-paid-for technical reports. How many Shell directors live at the Barendrecht CO_2 storage site? The people who do live there intuitively distrust statements made by someone who does not run any risk themselves. This distrust is justified. Studies show a strong correlation between the safety of technological systems and their geographic proximity to political and economic elites. The farther away the elites live, the less safe the technology tends to be.[35]

2. Exchanging views on risk

In addition to demonstrating that 'we are in this together' there are well-known practices that build rather than destroy trust between politicians and citizens. It is actually striking to see how little government experts and politicians care for the latter. The fact that not everything is 100% safe is rarely conducive to a discussion. On the part of politicians and administrators it leads much too often to unhelpful comparisons[36], such as tobacco kills more than nuclear plants. Such patronizing messages undermine rather than build trust in government's ability to deal with risks.

What is sound risk communication then? For instance, we know that being clear about your intentions and making them the central stage of your communication effort will create goodwill. We also know that coming across as honest, competent, fair and efficient is central to people accepting that you may have to make tough decisions for them[37]. As

34 Dutch Energy Council, "Eisen CO_2-opslag Barendrecht worden verscherpt" ["Requirement for CO_2 storage Barendrecht tightened"], available on the Internet at <http://www.energieraad.nl/newsitem.asp?pageid=15671> (last accessed on 16 July 2012).

35 Charles Perrow, "The limits of safety: The enhancement of a theory of accidents", 2 (4) *Journal of Crisis and Contingencies Management (1994)*, pp. 212–220.

36 Risk comparisons are known to be tricky. To avoid confusion they require formal analysis to ensure that defensible comparisons are being made and dedicated empirical research to ensure that the result is understood as intended. See on the subject Baruch Fischhoff, "Risk Comparisons", 2007. Paper 64. Available on the Internet at <http://repository.cmu.edu/sds/64> (last accessed on 16 July 2012).

37 Ortwin Renn and Debra Levine, "Credibility and trust in risk communication", in Roger E. Kasperson,and Pieter J. Stallen (eds), *Communicating Risk to the Public: International Perspectives*, (Amsterdam: Kluwer, 1991).; Ragnar E. Löfstedt, *Risk Management in Post-Trust Societies* (Basingstoke: Palgrave, 2005).

Renn's once highlighted, institutional performance is key to trust and credibility[38].

Politicians can no longer afford to just talk and not listen. Fischhoff's eight development stages in risk communication suggest that the time is long past when authorities could provide and explain numbers to the public and assume that this would be enough. Showing people the benefits in order to seek their buy-in, which has often been the next stage, is not enough either. The kind of risk communication that satisfies the parties involved needs to take the form of a two-way process. And to work best this process should also be non-persuasive. In a nutshell: treating people with respect and making them partners is a far more productive option for politicians than delegating risk communication to the 'ignorant smiles of the PR types'. As PR is often 'a good tool for digging oneself into a hole[39].

3. Persuasiveness of the fatalistic message

Resignation to certain risks, however small, is rhetorically effective only if the organization suggesting such resignation bears the risk itself. To illustrate, in 2009 during the Christmas mass, a deranged 25-year-old woman assaulted Pope Benedict. An elderly cardinal broke his hip in the commotion, but the Pope himself was unharmed. After the incident an Italian archbishop said, "Nothing serious happened. It was a woman who tried to greet the Holy Father.'[40]

What determines whether a message is effective in electoral terms? We often think of voters as having clear and outspoken emotions about politically contested issues. But according to psychologist Drew Westen, voters usually have conflicting feelings, and ambivalence is actually the norm. Powerful messages, says Westen, bring out these conflicting feelings. We apply moral principles to link these conflicting feelings and translate them into a political action.[41]

People have conflicting feelings about safety risks too. Take the attacks on airplanes. Of course these arouse anxiety and a nagging sense that danger can never be completely ruled out. Yet, few of us have become unwilling to fly for this reason, or step into the plane paralyzed with fear. This means that other emotions are at work as well. Resignation, anger, maybe even annoyance at all the upheaval.

Today's political messages do nothing with that ambivalence. They appeal only to the fear and promise protection – with the inevitable caveat that 100% safe is impossible. In 2004, two and a half years after 9/11, Senator John McCain, the then Republican US presidential candidate, formulated an alternative message:

> "Fly on the damn plane! Calculate the odds of being harmed by a terrorist! It's still about as likely as being swept out to sea by a tidal wave. Suck it up, for crying out loud. You're almost certainly going to be okay. And in the unlikely event you're not, do you really want to spend your last days cowering behind plastic sheets and duct tape? That's not a life worth living, is it?'[42]

McCain didn't deny the risk. He linked it with a principle: Braving the danger is a badge of courage and a way of life. With this he offered every television viewer a choice between a cowardly existence and a more heroic life. In other words, the very acceptance of risk is coupled to an appealing moral value – courage – and offers a way to increase self-respect.

Principles like this are required to break government's routine of overblown reactions to threats. They give the acceptance of risk a meaning other than docile resignation to fate. That meaning can take various forms. McCain presents acceptance as fortitude, as a form of superiority over the enemy.

VII. Conclusion

Philosopher Jos de Mul writes of the return of fatalism in the way we confront our destiny.[43] Everywhere there are situations where human intervention has come up against limits and triggered unintended effects. These are sometimes made explicit in politi-

38 Ortwin Renn, *Risk Governance; Coping with Uncertainty in a Complex World* (London: Earthscan, 2008).

39 Baruch Fischhoff, "Acceptable risk: A conceptual proposal", *Risk: 1 Health, Safety & Environment*(1994) :pp. 1–28,.

40 BBC News, "Vatican admits pontiff vulnerable to assault in public", available on the Internet at <http://news.bbc.co.uk/2/hi/europe/8430621.stm> (last accessed on 16 July 2012).

41 Drew Westen, *The Political Brain: The Role of Emotion in Deciding the Fate of the Nation* (New York: Public Affairs, 2007).

42 John McCain, *Why Courage Matters: The Way to a Braver Life*, (New York: Random House, 2004), pp. 35–36.

43 Jos de Mul, *De domesticatie van het noodlot: De wedergeboorte van de tragedie uit de geest van de technologie [The domestication of fate: The rebirth of tragedy out of the spirit of technology] (Zotermeer: Klement, 2006).*

cal decisions as well. An example is the, now partially dismantled, Dutch policy of tolerance towards the use of soft drugs. Tolerance in this case is an admission of our powerlessness to enforce the law, to eliminate the drugs trade. Yet at the same time the doctrine of tolerance assures us that by accepting our powerlessness we can prevent more serious harm, such as an escalation of drugs-related criminality.

Whatever form the message takes, one element is vital: it must be clear that the inability to prevent harm is not the same thing as helplessness or passivity. On the contrary, acceptance of powerlessness can provide a way to effective action. Thus powerlessness is transformed into power.[44] The idea is not to deny powerlessness or pledge that it will be resolved. Rather, acceptance of the inevitable is taken as a new and more constructive point of departure for government, politicians and public administrators when dealing with risks and incidents.

44 We thank Liesbeth Noordegraaf-Eelens for this observation.