UACES 45th Annual Conference

Bilbao, 7-9 September 2015

www.uaces.org

Bypassing the disciplinary power of data protection

Dr. Matthias Leese
University of Tuebingen

Paper prepared for the UACES Annual Conference, Bilbao, 7-9 September 2015

"90% of all crisis management has to do with information processes." (Interview, 11 May 2015) Security practices and data are inextricably enmeshed – thus having sparked intense discussions about surveillance, social sorting, preemption/prevention/precaution, predictive policing, and other efforts to act upon the unknown future in order to intervene into it. In other words: data have been rendered key to cancelling out the next event that threatens to unsettle our security, and data-based security practices have thus commanded critical attention (e.g., Amoore, 2011, 2013; Amoore and de Goede, 2008; Leese, 2014; Lyon, 2003; Rouvroy, 2013). This paper engages a different aspect of the temporal continuum of security production. Informed by a series of open, qualitative interviews with experts from European crisis management (predominantly practitioners, but also senior level ministerial representatives, researchers, and designers) that was conducted between April and June of 2015, the analysis emphasizes the role of information *during* a crisis – regardless of whether it would be caused by natural events (e.g., forest fires, floods, or storms), by accident/failure (e.g., industrial or nuclear incidents, blackouts), or by deliberate attacks (e.g., terrorism).

Distinct threat ontologies become leveled throughout crisis management by the urgency of intervention – an intervention that, as the above quote aptly demonstrates, hinges to a large extent on the availability of data on the event itself, on the topography of the affected area, on first responders and equipment, on weather conditions, on the affected population, on infrastructure, and on a plethora of other factors that can be key for effective mitigation of harm. As availability and timeliness of reliable information play such a key role for crisis management, major efforts have recently been undertaken to develop and design 'common operational picture' and 'common information space' IT solutions in order to ensure the interoperability of involved organizations, particularly when it comes to wide-ranging, transnational crises. Such formalization of information flows throughout cross-national digital infrastructures – widely considered a viable remedy for crisis management – is however, as the empirical accounts from the field itself have shown, coined by one major caveat: data protection. The legally binding status of data protection in fact produces a disciplinary power that unfolds unprecedented side effects when it comes to managing actual crises.

The argument that I seek to spell out here along the empirical analysis of expert accounts is the following: the European data protection framework as well as national data protection legislations provide detailed and specific regulations concerning the collection, storage, processing, and transfer of data, and particularly when it comes to personal data. To be perfectly clear from the outset: this is a good thing, and this notion is shared by most interviewees as well. However, as became clear from the experts' accounts, data protection in crisis management does in fact produce what might best be described as an 'informational straightjacket.' While experts and practitioners widely consider data protection necessary and valuable, they are at the same time confronted with what I call here the *disciplinary power of data protection*. In other words: data protection heavily interferes with what experts framed as necessarily efficient and swift information exchange between first responders and other involved agencies. Subsequently, the regulating force of data protection produces creative practices of bypassing official IT infrastructures that are supposed to facilitate cooperation in crisis situations.

The paper proceeds by briefly sketching out the current trends of interoperability in security practices and the ensuing efforts to design 'common operational picture' and 'common information space'

solutions. Subsequently, it engages the experts' accounts of the problems created through attempts to formalize information flows in crisis situations through IT infrastructure, thereby engaging empirical examples of creatively bypassing such infrastructures. Finally, I will reconsider the 'conflict' of privacy/data protection vs security in light of the disciplinary power of data protection.

Methodological note

This paper has emerged in an inductive fashion through the collected empirical material. While the expert interviews were originally conducted for the purpose of identifying ethical stakes in crisis management in order to counsel the development of a common information space within the project consortium, initial analyses of the material revealed the strong narrative about data protection that was put forward by all respondents when talking about problems that they encountered in their everyday practices, thereby rendering the topic at hand a compelling thematic that I chose to pursue. The argument throughout this paper will accordingly be spelled out closely along the experts' accounts and their perspective on the role of data and data protection within their professional field. I have therefore decided to give the interview material itself the necessary space, as the examples put forward by the interviewees in many cases speak powerfully for themselves.

Let's share! Interoperability in crisis management

"We need data in order to make decisions and in order to make good decisions." (Interview, 16 April 2015) Crisis management is however not only about data and information as such, but at the same time one of the major stakes of the field is how to share data. Complex contingencies with multiple involved organizations practically command a seamless information flow, as no organization can gather and process all necessary information by itself, nor can it subsequently act upon it in an isolated fashion. In very simple terms: crisis management is about working together, about cooperation and exchange. Using the current buzzword: it is about interoperability. Questions of interoperability – or rather, a presupposed lack of interoperability – have been high on the European security agenda for quite some time. Interoperability, as has been highlighted by several diagnoses, is widely regarded necessary in terms of crime prevention and policing, in terms of counterterrorism, in terms of migration and border control, and in terms of effective crisis management.

The European Security Research and Innovation Forum (2009: 9), a group of high-ranking security experts, practitioners, and industry representatives, recommended that in order to improve security, "research must cover technical interoperability aspects between deployed systems, as well as interoperability at the organisational level, taking into account the diversity of cross-border cultures." This recommendation falls well in line with ongoing efforts of streamlining information flows and enhancing data exchange in crisis management. Such a need has also been reinforced by the European Network and Information Security Agency (2012: 14), stating that a "lack of interoperability between first responders and communication problems are the most common findings in post-crisis lessons learned exercises." The OECD (2004: 13), in a report on large-scale disasters, has argued that "vital elements of the picture are scattered across central and local government, law enforcement and regulatory authorities, corporations and other stakeholders in the sectors concerned, from citizens to hospitals."

Similar arguments can in fact also be found throughout academic engagement with crisis management. As Rhinard et al. (2013: 250) state, "concrete cooperation is hampered by different risk and threat assessments, incompatible response methods, late 'situational awareness', a lack of common technical standards, and slow deployment and low interoperability of resources," and 't Hart and Sundelius

(2013: 453) add that "robust sense-making capacity, in other words systematic ways of sorting, accessing, prioritizing and communicating information, is imperative to prevent both operational-responders and strategic policy-makers becoming overwhelmed and making costly mistakes through misunderstandings and miscommunication." Current efforts to improve crisis management thus culminate, as Comfort (2005: 348) summarizes, in the "need for interoperability of the highly diverse, large-scale networks of communications and information exchange used by public, private, and nonprofit organizations to provide societal services."

This discourse is also well reflected in the experts' accounts of their professional experience. Interviewees unanimously agreed that there is an inherent need to share data and information, as well as a need to better structure and make sense of data. As one interviewee framed the current stakes within crisis management:

> Actually there's a real absence of some common working practice or common working methodologies between different organizations as well, but we have also been focusing in the last couple of years on actually trying to establish some joint coordination structures across our emergency services to better enable or be up to receive, as it were, all of the information and then actually take some decision based upon it. (Interview, 22 May 2015)

This does of course not mean that organizations are only beginning to cooperate – far from it. However, cooperation among involved actor was often found to be eclectic, uncoordinated, and heavily reliant on the professional networks of particular individuals within involved organizations. Moreover, with the unprecedented increase of available digitized information from large-scale, interlinked databases, satellites, and many different sensors, it turned out that the IT infrastructures in place were not able to process incoming information flows from other organizations in a satisfactory fashion. As one expert framed the problems:

> We found in [country] that the police, ambulance, and fire services were all operating on totally different systems, totally different ways of responding, all sorts of things were totally different. And we had a whole project here on interoperability, trying to get them all on the same communications network, all on the same level of interchanging information. […] So at that level, there are people here who have done a huge amount of work to try and get that in place. (Interview, 24 April 2015)

Another expert, speaking for a different national context, explained what kind of problems are caused by a lack of interoperability when it comes to dealing with actual crisis situations:

> The forest fire we had last year up in [country], I was there during the fire. And when I was there, during the first week, they had problems of developing a working system for information sharing within the central command. Like, within there was a building and in that building we have representations from different organizations, you have the senior commander from the rescue services and so on. And you have the military, you have the healthcare, the police, you have the municipality, several municipalities, you have County Administrative Board representatives and so on. And they needed to share information. […] And they didn't have a joint system for sharing that information. (Interview, 16 April 2015)

The lack of the capacity to actually share information was only described as one part of the problem, though. The other part, equally as important, is to find a suitable way to structure information flows, to process data, to visualize it and to make it accessible – in short: the capacity to make sense of data. Without such sense-making, the availability of information would be rather useless, and crisis situations could not be more effectively handled than before, thereby rendering the promises of the digital age rather useless. As one interviewee framed it, data sharing can in fact quickly turn into data overload:

> Sometimes there is no lack of data. There's so much data. But what you do with the data is the challenge. How do you deal with the data? If you look at it from a hindsight perspective, you see: there were a lot of data. But what do you do with it? And the processes of how to deal with the data are very important, I think. Also from a technical perspective: could we sort the data, could we sort it out could we structure the data in one way or another? (Interview, 16 April 2015)

Added another expert:

> The requirement […] is to get something which is interrelated, interacting, up to the minute, taking into account all the new technology that's coming in. Because, I mean, of all the things we've talked about, this kind of satellite imagery and use of satellites and things like that, these days we get that into it. There is so much data coming in, there's a need to have some way of everybody being up to use it, you know. From the local level to the national level, but equally that it's up to date and people can make decisions based on all of it, not just on the little bits that they get in different times. (Interview, 24 April 2015)

Even though interoperability needs to cover both organizational aspects (e.g., using a shared terminology, establishing a common taxonomy, having coordinated goals, etc.) and technical aspects (European Commission, 2005; European Security Research & Innovation Forum, 2009; Roßnagel et al., 2012), the emphasis here is clearly put on the technical capabilities for organizing and processing cross-agency information flows. This tendency is well-reflected in current efforts to develop and design 'common information spaces' and 'common operational pictures' that are supposed to resolve the questions surrounding sharing and sense-making of data. The simple idea behind such approaches is that available data – not only geo-data, population data, infrastructure data, maps, etc., but also data from and about involved organizations – would be joined in some form of centralized portal, which would then be accessible for all involved organizations, thereby producing accurate support for the specific organization and the specific task at hand.

However, while in theory, experts and practitioners agree with such an idea, it also became apparent throughout the interviews that no clear vision of how to realize such a technological infrastructure in the best way possible exists as of yet. As one interviewee framed the issue:

> One of the discussions that we've been having is, you know, you share everything, put everything in the cloud, and then give whoever needs access to it can have it. (Interview, 8 June 2015)

> I suppose in very simple terms you've just got to imagine this giant pool of information that you can simply dip into and take out what you need. I personally think that it is going to be very difficult to try and define, let's say, sticking with the swimming pool analogy, to try and define the shape, the depth, the color of the tiles, the amount of water beforehand, because you're never quite sure what exactly you're going to need. What the missing pieces of the jigsaw puzzle are. […] Actually, what we probably need is a giant pool full of all the information-water we need, that I can just dip into and take out only what I want. (Interview, 8 June 2015)

The disciplinary power of data protection…

"I would say that the information sharing and the data aspects, whatever you like to call it, has changed the conditions for management a lot." (Interview, 16 April 2015) Enter: data protection. Data protection is primarily a legal term, and one that is located within a complex and quickly transforming field. Being the legal codification of the abstract concept of privacy, being constantly challenged by advances in information technology, and currently undergoing reform at the supranational level

through the EU data protection framework reform, the notion of data protection itself is somewhat messy and ambiguous (for an incomplete overview of recent discussions, see Bellanova, 2014; Gutwirth et al., 2014, 2015; Gutwirth et al., 2013), and to a large extent coined by uncertainties regarding key questions of data collection, storage, processing, and sharing. To be quite concise here: I do neither seek to engage the legal and philosophical discussions surrounding data protection here, nor do I seek to analyze the specific legal provisions when it comes to data protection and crisis management on the European level and in 28 different member states. What I am rather interested here are the effects that data protection unfolds on the field of crisis management itself. Throughout the analysis of the empirical material, it became clear that practitioners have quite ambivalent feelings when it comes to the role of data protection and its impact on their work practices. As one respondent pinpointed the arguably biggest hurdle:

> I think there's, you know, if you say personally identifiable information in a conversation, then you can almost feel everyone tense. It's just that nobody wants to run afoul of that. And no one is entirely sure how to avoid running afoul of it. […] And so it's seen, I think, frequently as rather rule-driven and therefore just one more damn set of rules that we have to keep in mind. And that does, I think, create some degree of friction and anxiety. (Interview, 2 April 2015)

His reference to friction and anxiety is indeed backed up by other accounts of how data protection is seen as a stepping stone both in conceptual terms as well as in concrete crisis management practices. Arguably, such anxiety stems from a lack of definite knowledge of what kind of data handling practices are allowed under specific data protection legislations, as well as from a lack of guidance on how to deal with questions of cross-border data sharing. Crisis management professionals are in fact well aware of the ethical and societal importance of privacy and data protection, and they are certainly eager not to violate any legal provisions – but not knowing exactly what kind of practices could cause such a violation, there is a deep insecurity about doing the right or the wrong thing. As said one interviewee:

> The idea of collecting data in local populations, the idea of data transport, what does that mean? Can you use a server in one country, for instance in country A for a test or an evaluation and in country B there is a server where the data is located? […] If we have the database in one country, and not in the country where the test is conducted, for instance [country], by doing so we wouldn't run into that problem. But at the same time it is highly technically and legally complicated. To be honest, I'm not sure whether we actually solved this problem so far. (Interview, 4 May 2015)

Such rather abstract problems would in the interviews regularly be backed with accounts of very specific, concrete experiences or scenarios that in fact emphasize the conflicting notions of data protection and crisis management. As one respondent described practical problems:

> Let's say that one of the water companies we have in [country] has a list of people who identified themselves being vulnerable so that in emergency they could be entitled to delivery of water. Under that system, they would not share that data with the health people. And so the health people would say: "We've got our own list of people who are on dialysis. Can we not check if that's the same as the list you have of people who need water for the dialysis system?" And so they are both refusing to talk to each other on the basis that it was confidential information. So in a sense it became a problem. (Interview, 24 April 2015)

As a reminder: the point here is not the data protection framework itself, but rather how it is perceived by professionals within crisis management. Through their perception of data protection as the dynamic and contested field that it is, data protection unfolds effects that go well beyond its narrow legal scope. What I chose to call here the disciplinary power of data protection can be made tangible through the

figure of the panopticon. As originally described by Bentham in 1791 (1995), the panopticon was an architectural model for a highly effective and efficient prison design. The basic idea here is to have one central watchtower in the middle of the prison building, offering an uninterrupted full circle view of the complete surroundings. The cell blocks would then be arranged around the central watchtower such that each and every one of them could be easily surveilled from the watchtower. Through such an arrangement, a prison could be effectively run with a minimal number of guards. However, the panopticon only gained its importance as a way of thinking about power and discipline when Foucault, in his book *Discipline and Punish* (1977) turned Bentham's original angle upside down.

Whereas for Bentham, the panopticon was to be read through the lens of the prison guards (i.e., the watchers), Foucault highlights the perspective of the inmates (i.e., the watched). Starting from the notion that for the prisoners in their cells, as they would not be able to see the insides of the watchtower, it would not be possible to determine whether they would be watched at any given moment, he develops the notion of a disciplinary effect that regulates the behavior of inmates regardless of whether they are actively being watched or not. As writes Elmer (2012: 23) in this regard: "Foucault's panopticon emphasizes an enactment of surveillance, a subjectivation of power, as instilled in prisoners who architecturally speaking must assume ubiquitous surveillance, that they may be under inspection at any time, night or day." Key here is the possibility of being watched that suffices for a regulation of behavior according to what is acceptable and permitted in a given social or institutional environment (in this case: the prison).

My argument here is that throughout the crisis management experts' accounts of data protection runs a similar notion that depicts data protection as an all-encompassing specter that haunts necessary working practices in terms of information exchange between organizations. In order not to potentially violate data protection legislation, crisis management thus undergoes change. The disciplinary effect that data protection unfolds in crisis management practices is however notably a different one from Foucault's notion of surveillance and behavioral adaptation – it is one that sits comfortably with the increased digitization of information exchange and the technologization of the field that has been rendered a remedy for pressing interoperability needs. The disciplinary power of data protection becomes inscribed within the formalization of the very IT infrastructure that is supposed to facilitate information exchange, thereby creating curious effects. As one expert described such effects:

> And when I look at these technologies in [country], especially this big common information space called [name], it has really strong information security protocols implemented to it. Because the whole idea is that organizations should be able to really share sensitive information and no one who shouldn't have access to the system will get access to the system. But in crisis situations that start small and then slowly escalate, or rapidly escalate, then you often need to invite new people into the information flow. But this system, it seems like they totally ignored the fact how social media platforms work. So, it's very difficult for me to send an invitation, if I would like to send an invitation to you, because I want you to be part of my team. So they don't have some sort of sending invites in order to quickly allow others to get some sort of access. But, instead then I have to call the support, fill in some sort of standard forms and then they will evaluate if you should be allowed to have access to the system. Then we will need to send you some sort of digipass, so you can in a safe way log into the system, or a secure way. And then, obviously, people will not use this system, because it's so difficult to include people that you would like to include. (Interview, 30 April 2015)

IT infrastructures must obviously adhere to legal regulations – as stated earlier, crisis managers appear to be well aware of the necessity for privacy and data protection and approve of it in general – that however unfold in strict procedural formalization and a heavily rule-based use of technical solutions

of information exchange. This goes in fact as far as effectively undermining established crisis management practices. As one interviewee framed the problematic:

> I think the biggest stumbling blocks, as always, are going to be the law and the ethical behavior sides and so on. It got to the stage where you can't give somebody somebody's name because that would be identifying them, obviously, and all those kinds of things. […] Those rules themselves are not clearly defined. There's cases all the time on what constitutes personal information. […] And the other thing is, that in itself it is an area that is only going to get more restrictive. (Interview, 8 June 2015)

…and its creative bypasses (for the greater good)

"We find it can be detrimental, whereas I'm sure they meant that to be a good thing. But you and I didn't see each other's information." (Interview, 24 April 2015) Crisis management is inherently good, and so is privacy and data protection. How to resolve the apparent conflict between two principles, then? As there seems to be no easy way to reconcile data protection and the need for information exchange, experts surprisingly gave account of highly idiosyncratic workarounds in concrete crisis scenarios, thereby bypassing official IT infrastructure throughout creative repurposing of everyday technologies. Returning to the account of the forest fire already presented above, the interviewee goes on to describe how interoperability was eventually created ad hoc as the crisis situation continued to unfold:

> And then there came, it was a guy from a volunteer group […], he showed up and he said: "I'm quite skilled with computers." And one of the commanders from the rescue services then said: "Okay, can you help us?" So he set up, I think it was a Google account, Gdrive or whatever it was. Like a server. And he arranged an internal information sharing system which I used. I'm not sure if you could call it an information sharing system, but more like a system for data storage, and yeah, a bit of sharing as well. So they had Gmail accounts, they had like a server, which you could use for logging and so on. Then it worked for like a couple days, it worked well. Everyone was happy with that and then came, I think, some IT security guys. They got to know what was going on, and they said: "We can't do this. It's not secure at all." So they actually re-arranged the IT structure within the joint command group […] in a more proper way, according to security thinking. But it didn't work as good as the Gmail or Gdrive thing. (Interview, 16 April 2015)

Added another expert with reference to the organizational practices during that fire:

> That was the biggest forest fire ever experienced, that we have had in [country]. And it was really a big operation. But, very few of the standard information systems were used in organizing the work. The big [name] system, which is a common information space that is in use in [country], was not used. And also more local logging or reporting systems from the fire rescue service, for example, were not used. Instead, they invented a new common information space based on Gmail addresses and Gdrive, basically. (Interview, 30 April 2015)

Another empirical example describes a similar case in which the capacities of official IT infrastructure did not cover the operational needs of information exchange, thus leading to a creative workaround incorporating mobile phones:

> We've had a similar experience in [country] with the radio system, the airwave system. Because obviously tetra was not very good at working with lots of data, so most police forces have gone to commercial suppliers and they're using Blackberries, or whatever it might be for the data. And one of the issues is the security people saying "You can't do that", you know. And chief constables have had to say: "Unless you can give me another solution, thanks for your advice,

> but I have to do something. I can't just sit there and not do anything because all the rules say you can't do this, you can't do that, you can't do the other. I've got to make a pragmatic decision and say right, I accept there is some security issues, I'll do what I can do to mitigate those, but I've got to do something." (Interview, 8 June 2015)

The common notion that runs through these examples of workarounds is arguably not a malicious one. As has been shown so far, crisis managers do not seek to deliberately infringe upon individual privacy, but they seek to place data protection within the wider frame of their professional obligation to protect the population, to mitigate harm, and to save lives. However, since – so the argument I put forward here – the disciplinary power of data protection has been inextricably enmeshed within their professional tools, they come up with creative solutions for working around ethical and legal conflicts. Even within such creative and idiosyncratic practices, practitioners are however still aware of the implications for privacy and data protection. As said one respondent:

> [It] is really, from my point of view, fascinating, how they actually were able to create something new during the management of the operation. On the other hand, I'm a bit frightened also that these American platforms were used in when [country] governmental organizations are dealing with the most complex situation they have dealt with the last few years. I mean, I'm not even sure it was legal to use Gmail and Gdrive, because then governmental information is stored on servers, located perhaps outside of the EU. (Interview, 30 April 2015)

Most notably, practices of creative repurposing commercial/private technologies for the sake of crisis management provide a possibility to circumvent formalized logging of actions during crisis situations through which data protection violations could later be retraced. As explains one expert:

> With the fire and rescue services, the most important tool for information sharing was the cell phone. And this was during a time when a separate, tetra-based system was implemented in [country]. But what we saw was that the cell phone was the primary vehicle for reporting, verbal reports and so on, because it allowed the incident commander to include various actors in a very simple way and it was this very free material or free infrastructure with flexible characteristics in a sense. But the problem of providing verbal reports is that they are ephemeral and not persistent. So what I argued was that we should pay more attention to the social networks that are created on an accident site and also start to record these conversations, so that we can transcribe them, because it's basically these social interactions, mediated by cell phone calls, where the true information flow exists, and not in the formal reporting system. (Interview, 30 April 2015)

There is however a second, non-data protection related narrative running through the empirical material when it comes to the circumvention of official IT infrastructures in crisis situations. As crises usually occur in a very low frequency, practitioners are seldom familiar with the use of specific IT tools for crises. Technology, so the argument put forward by respondents, must however be frequently used in everyday contexts, because otherwise there will be a lack of familiarity in actual crisis situations that leads to a neglect of, for instance, a common information space tool, simply due to a lack of user capabilities. As one expert explains that problematic:

> When I'm used to having contact with my cell phone, I will do it in this specific situation as well. And you can say: "Ah, then you have to have other instruments, blablabla." But they won't work! It's a fantasy world. It's a world of organizations who earn money for specific things. But I really think that Apple and Google and Microsoft are far more important than all those specific things that we make for specific situations. (Interview, 11 May 2015)

In the end, practitioners in fact engage in a moral evaluation takes into account different factors such as ethics, the law, and their professional as well as personal desire to do the right things during a

situation in which the decision to compromise the efficiency and effectiveness of operations due to complicated procedures and legal constraints can hamper the possibility to mitigate harm. As one interviewee gives an account of such a moral evaluation that indeed takes into account the consequences that could occur from data protection violations:

> I understand the law, I understand my obligations and the powers that I hold […] but then I don't see how you can create a system that will make me behave ethically. Because I wouldn't be taken to court for example, and prosecuted, for behaving unethically. As far as I'm aware, there's no offense really that covers that. I could be disciplined for improper disclosure of information. Telling people things that they shouldn't have been privy to. But I don't see how a machine can prevent me from doing that. Because if I acquire some information from this common information space that I'm entitled to and I need to know, there's nothing to physically stop me turning around and saying to someone else who shouldn't know: "Hey, guess what I've just found out." (Interview, 8 June 2015)

Reconsidering data protection and security

"Information sharing between professional agencies is – there are some problems, definitely. There are problems. But when the shit hits the fan, when you have it in reality, I think it's not a very big problem." (Interview, 16 April 2015) The relationship between privacy and security has long been framed as an incommensurable conflict or, at best, a trade-off. Even though such a conceptualization is neither epistemologically nor logically coherent, it has been quite persistent (Friedewald et al., 2010; Leese, 2015; Valkenburg, 2015), and it can be retraced to the emergence of the field of European security research itself, being coined by strong industrial interests and representation (Bigo and Jeandesboz, 2010). Privacy, and its legal derivative data protection, in this vein was framed as hampering the effectiveness and efficiency of data-driven security measures.

The relationship between data protection and security sketched out throughout this paper is a slightly different one, however. First of all, it must more precisely be described as a conflict between data protection and interoperability – a concept that is widely regarded key for successful crisis management, and one that hinges precisely on practices of data collection, processing, storage, and sharing. Those practices are in turn regulated by EU and national data protection frameworks, thereby creating a set of mandatory legal provisions that regulate crisis management in concrete crisis situations. Thus, friction arises. As one interviewee clearly put forward:

> The basic idea is that data protection is something that you should take into consideration, in some form or another, right? And of course you can prosecute data protection violations by way of compensation claims and so on. […] You could also frame it as a violation of fundamental rights, but nonetheless there's a tension between data protection and civil protection. (Interview, 9 June 2015)

The existence of the conflict itself is not necessarily a novel insight. In fact, governments as well as academia have acknowledged the tension between data protection and interoperability. As for instance a British guidance report for crisis management points out with regard to data protection: "Its job is to balance individuals' rights to privacy with legitimate and proportionate use of personal information by organisations. In the context of emergency planning – and, in particular, in the aftermath of an emergency – it is important to look at this balance critically and realistically. […] We must all work within the law, but in the circumstances set out in this guidance, we feel that uncertainty should not be used as an excuse for inaction when it is clearly in the interest of individuals and the public at large to act positively." (HM Government, 2007: 2) Such efforts will arguably become more important in the future. As Finn et al. (2015) argue, "as time progresses and crisis managers,

humanitarian organisations and others' engagement and activities and interaction with big 'crisis' data grows, it will be necessary to implement appropriate measures and policies to manage, protect and optimise the value that can come from engaging with this data."

And while research and guidance on how to possibly reconcile data protection and interoperability are necessary and must be valued as such, it remains somewhat questionable whether they will be able to resolve the effects of the disciplinary power of data protection. As I have argued along the expert accounts of crisis management practices, a key characteristic of data protection law is its complexity and dynamic nature which is at times hard to grasp even for data protection lawyers. Practitioners of crisis management in fact feel a strong insecurity – even anxiety, as one respondent framed it – about questions of data protection. An insecurity which in turn produces creative, ad hoc bypasses that are imposed on crisis managers by the perceived disciplinary power of data protection.

The relationship between data protection and security, read through this particular lens, must therefore be adjusted. While it had long been argued that, on an abstract level, the need for security would easily trump the need for privacy, concrete security practices in light of concrete data protection legislation paint a slightly different picture. Due to its legally binding status, data protection appears to have ousted the notion of privacy when it comes to data collection, processing, storing, and sharing. Data protection in fact unfolds a disciplinary power that is capable to subdue even security practices – and if only in the particular field of crisis management. Governments are still eager to frame the relationship between concrete practices and concrete legislations as a 'balance', but it remains questionable who would then be entitled to define the nature of such a balance. It might very well be the case that this question would be relegated to the courts, thus contributing to a further 'legalization' of crisis management practices. Data protection has thus emerged not only to be a concrete forum for discussing privacy and/vs security, but also as a means to govern security.

Conclusions

This paper has retraced the status of data protection within the professional field of crisis management. I have thereby argued that the legal specifications of data protection stand in contrast to obligations of sharing information between involved organizations in crisis management operations. While it might in fact be possible to reconcile data protection legislation and professional working practices within crisis management, the paper has instead highlighted the unprecedented side effects that data protection imposes on involved actors. Through the accounts of experts from the field, it has become apparent that the complex nature of data protection in fact unfolds a disciplinary power similar to surveillance effects within the panopticon model. In other words, when crisis managers are not sure about how to handle data protection, they tend to creatively bypass data protection in order to avoid possible violations of the legal framework. Notably, questions of familiarity with specific IT infrastructures play a role within such practices of bypassing as well – however as has been shown, data protection becomes deeply enmeshed within 'common operational picture' and 'common information space' solutions, thereby unfolding narrow limitations for information sharing during crisis. As a consequence, practitioners try to escape the disciplinary power of data protection through creative repurposing of private and/or commercial technologies such as Gmail/Gdrive or Blackberry phones, thereby undermining the otherwise strong institutional position of data protection.

Acknowledgments

The empirical research for this paper was funded by the European Commission under grant agreement no. 607821.

References

't Hart P and Sundelius B (2013) Crisis Management Revisited: A New Agenda for Research, Training and Capacity Building Within Europe. *Cooperation and Conflict* 48(3): 444-461.

Amoore L (2011) Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society* 28(6): 24-43.

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability.* Durham/London: Duke University Press.

Amoore L and de Goede M (eds.) 2008. *Risk and the War on Terror,* London/New York: Routledge.

Bellanova R (2014) Data Protection, with Love. *International Political Sociology* 8(1): 112-115.

Bentham J (1995) Panopticon. In Božovič M (ed.) *The Panopticon Writings.* London: Verso, 29-95.

Bigo D and Jeandesboz J (2010) The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5. Available at: http://www.ceps.eu/system/files/book/2010/02/INEX%20PB5%20e-version.pdf (accessed 7 July 2014).

Comfort L K (2005) Risk, Security, and Disaster Management. *Annual Review of Political Science* 8(1): 335-356.

Elmer G (2012) Panopticon-Discipline-Control. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 21-29.

European Commission (2005) COM(2005) 597 final. On Improved Effectiveness, Enhanced Interoperability and Synergies Among European Databases in the Area of Justice and Home Affairs. 24 November. Brussels.

European Network and Information Security Agency (2012) Emergency Communications Stocktaking: A Study Into Emergency Communications Procedures. Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/emergency-communications-stocktaking/at_download/fullReport (accessed 26 May 2015).

European Security Research & Innovation Forum (2009) ESRIF Final Report. Available at: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (accessed 7 July 2014).

Finn R, Watson H and Wadhwa K (2015) Exploring Big 'Crisis' Data in Action: Potential Positive and Negative Externalities. Paper presented at ISCRAM Conference, Kristiansand, 24-27 May.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Friedewald M, Wright D, Gutwirth S and Mordini E (2010) Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework. *Innovation: The European Journal of Social Science Research* 23(1): 61-67.

Gutwirth S, Leenes R and de Hert P (eds.) 2014. *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges,* Dordrecht/Heidelberg/New York/London: Springer.

Gutwirth S, Leenes R and de Hert P (eds.) 2015. *Reforming European Data Protection Law,* Dordrecht/Heidelberg/New York/London: Springer.

Gutwirth S, Leenes R, de Hert P and Poullet Y (eds.) 2013. *European Data Protection: Coming of Age,* Dordrecht/Heidelberg/New York/London: Springer.

HM Government (2007) Data Protection and Sharing - Guidance for Emergency Planners and Responders. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf (accessed 10 August 2015).

Leese M (2014) The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union. *Security Dialogue* 45(5): 494-511.

Leese M (2015) Privacy and Security - On the Evolution of a European Conflict. In Gutwirth S, Leenes R & De Hert P (eds.) *Reforming European Data Protection Law.* Dordrecht/Heidelberg/New York/London: Springer, 271-289.

Lyon D (ed.) 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination,* London/New York: Routledge.

OECD (2004) Large-scale Disasters: Lessons Learned. Available at http://www.oecd.org/futures/globalprospects/40867519.pdf (accessed 15 June 2015).

Rhinard M, Hollis S and Boin A (2013) Explaining Civil Protection Cooperation in the EU: the Contribution of Public Goods Theory. *European Security* 22(2): 248-269.

Roßnagel A, Engelbach W, Kurowski S, Zibuschka J, von den Abeele D, Isbert V, de Jong A and Vullings E (2012) SECUR-ED Deliverable 22.1: Interoperability Concept.

Rouvroy A (2013) The End(s) of Critique: Data-behaviourism vs. Due-process. In Hildebrandt M & de Vries K (eds.) *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology.* Milton Park/New York: Routledge, 143-168.

Valkenburg G (2015) Privacy versus Security: Problems and Possibilities for the Trade-Off Model. In Gutwirth S, Leenes R & de Hert P (eds.) *Reforming European Data Protection Law.* Dordrecht/Heidelberg/New York/London: Springer, 253-270.