ephemera
theory & politics in organization

ISSN 1473-2866 (Online)
ISSN 2052-1499 (Print)
www.ephemerajournal.org
volume 17(2): 65-84

On anonymity in disasters: Socio-technical practices in emergency management

Katrina Petersen, Monika Büscher and Catherine Easton

abstract

Disasters are often thought of as exceptions to the norm, where it is ethical to break rules in order to maintain social order and security. Indeed, such exceptions are recognised in high-level international legal provisions such as the European Union's (EU) Data Protection Regulation, building the expectation that during disasters systems of data sharing and protecting, including anonymity, will have to balance the urgency of the situation, the effort to manage those regulations, and the risks being faced in order to provide the security these protections intend. This paper explores what this means for the practice of anonymity as it examines the tensions between the social and technical practices behind information sharing for disaster management. By examining anonymity as a practice both in relation to how information is sourced from a community being protected and to how information is shared between organisations doing the protecting, this paper opens up the black box of information sharing during disasters to begin to unpack how trust, community, liability, and protection are entangled. As disaster management exposes and juxtapose social and organisational elements that make it work, we find that what anonymity means, and the security and protection anonymity offers, creates a mélange of hope of unprejudiced reception, protection from liabilities, opportunities for shared meaning, limitations to solidarity, reinforcement of power struggles and norms, and the ability to mask difference.

Introduction

During an interview about how he manages data quality when disaster information comes from a range of sources in a variety of formats, an experienced police chief from the UK offered up this statement:

> I'll be very reluctant on an anonymous call from someone who didn't want to tell you anything to jump straight to that action point. It comes back to developing your intelligence first. (Police Chief, UK in May 2015)

Expressed almost as an aside within the comments, he points to an important issue in the social productivity of anonymity: disaster intelligence is built around knowing who your information comes from; it is built around being able to link information to a person. Yet, in today's environment of digital information sharing for disaster response, anonymity is not just a privilege, it is a regulated right. Sharing disaster information through digital infrastructures puts into tension these social and regulatory practices and makes visible the complex ways in which anonymity produces power in society. As these information practices engender new interactions between groups sharing the data, new ways of seeing informational needs, and new methods by which to get involved, the role of anonymity in these socio-technical relations becomes less straightforward and clear. Considering the increasing move towards information technology solutions to building new formal collaborations and forms of responder interactions during disasters, this power needs to be considered in greater depth.

Anonymity grants specific forms of power both to those providing the information and to those acting upon it. This is because the ability to be anonymous instigates specific social and technical ways of organising around and within a given emergency situation. Anonymity is often practised when there is fear of discrimination, namely when there is a fear that information from one source might get privileged over another (Nissenbaum, 1999). But the equity it provides is only as good as the consistency in practices and the consistency of the contexts in which it is made available and engaged with. Without such consistency, having no identifier at all can inspire more questions rather than fewer and lead to greater distrust (Fast, 2014). This can be a challenge when quality assurance comes primarily from socialisation practices, affecting not just how information is understood by a responder, but also affecting how information is classified and made accessible or notable as it moves onto digital sharing platforms.

In this paper, we explore practices of digital disaster information sharing to better understand the work done, both socially and ethically, by acts of anonymity. We start from a single premise: anonymity is neither a state nor something that can happen in isolation, but emerges along with specific forms of social interaction and organisation. Taking a perspective that spans the disciplines of mobilities studies, science and technology studies, and legal studies, we argue that these practices of anonymity in relation to socio-technically shared information are more than just key components in inter-organisational practices and approaches to disaster management. Practices of anonymity are also intimately intertwined in civil community building and maintaining practices, such as the ability to produce

shared meaning, to produce states of privilege or equality, and to produce spaces for negotiating difference.

In order to best examine the tensions that emerge around the social productivity of anonymity in disaster information sharing, we examine the design and uptake of new information sharing technologies and practices for disaster management, processes that directly influence how those engaging in disasters are organised. Our research has been carried out in a European Union (EU)-funded research project (SecInCoRe.eu), concerned with the collaborative design of technology to enable inter-organisational information sharing for disaster management. In this project we work with engineers and practitioners to experiment with the design of new forms of disaster information sharing that can support more ethically and socially reflexive organisational practices. Our research, conducted from 2014-2016, includes data from interviews with emergency practitioners from across Europe, ethnographic observations of disaster training exercises, and multi-day collaborative design workshops. The practitioners with whom we have worked come from a range of backgrounds, including fire and police officers, community resilience planners, information technology managers, departmental liaisons, and national security experts. The slices of disaster explored are equally as varied: discussions of lessons learnt around past disasters, observations of training and planning practices based on expectations, experimentations with technological prototypes exploring what might happen next. There is no single disaster, single agency, or single country that drives this work. Our aim with this work is to think through the issues that are often contested and situated in order to help find ways to best support engineers and disaster practitioners as they design and use new technology to collaborate around disaster management. To do so requires building our empirical evidence in ways that reflect disaster information sharing practices, by engaging with amorphous and ever modifying communities.

We first explain the move in disaster management to digital information sharing that requires new approaches to anonymity. We then expand upon key definitions of anonymity and disaster in order to set the stage on which we are working. We follow this with an exploration of disaster information and anonymity in two ways. First, we examine how information that is anonymously sourced gets dealt with by those in disaster management and how that affects not only the relationship with the information but with the communities at risk. Second, we examine information sharing between disaster agencies and how anonymity both binds and excludes these organisations as communities of response emerge. Each discussion opens up different elements within the black box of information gathering and sharing during disasters. Through them we explore how the socio-technical production of anonymity produces a mélange of hope of unprejudiced reception, protection from liabilities, opportunities for shared meaning, limitations to

solidarity, reinforcement of power struggles and norms, and the ability to mask difference. We end with a discussion on the implications of these intersections on the social productivity of anonymity.

The social and data practices of disaster management

Disaster management involves a complex, non-linear cycle of planning, mitigation, response, and recovery. Cross-border disaster management and information exchange requires a certain level of interoperability between different organisations, their practices, and their technologies as they work through these phases. However, within this framework, there are a large number of crisis management models, with specific models created to cover a range of hazards, including natural disaster, terrorism, chemical spill, and medical epidemic. Moreover, these models evolve on almost a daily basis. This constant change is in part because of the situated nature of disasters: every disaster is grounded in a specific history of social order and socio-technical cultures of practice. Moreover, because of their innately disruptive character, disasters bring previously accepted analytical categories and systems of classification into question (Klinenberg, 2002; Oliver-Smith, 2002). But this is also because there are wide variations in response agencies' service delivery, both between agencies and within a given agency. For example, when discussing the police's role in disasters throughout the UK, one practitioner put it, 'so whilst we provide the same service, we do it in so many different ways that actually there is a commonality but it makes a very, very vague commonality' (Police Officer, UK in March 2015).

While there are certain common criteria between agencies and different situations, it is often difficult to be sure of consistency in interpretive practices and the consistency of the contexts in which information is provided. There is no routine to rely upon fully, there is no standard process or procedure that fits all circumstances, and (perhaps most importantly of all) the situation at the commencement of any incident, no matter how big or small, is rarely clear and complete. In some cases, as explained by a Fire Chief involved with the Federation of the European Union Fire Officers Associations, reliability and usefulness of information is defined in advance by Memoranda of Understanding (MOUs). In others, as explained by a senior Hazardous Area Response Team Liaison, UK, it is defined by the number of people who use a source. Or, as explained in interviews with officers in the Greek K9 bomb squads, while it is mandatory to check all information regardless of the reliability of the source, they often do so based on how the information is provided (e.g. speech pattern and tone of voice of the threatening phone call), the bombing target, and how long until the explosion. Interoperability between these practices cannot be assumed.

The one trend that appears in our interviews is that reliability and usefulness are based on trust, which is based on social networks: if you already know the person and they have been reliable in the past, then you trust the information that comes from them. Not knowing sources often leads to withholding initial trust. How these relationships are leveraged creates 'knowledge gaps'; gaps, as Frickel (2008) argues, that often lead to uneven spreads of risk and resources. This not only brings into question what it means to know a disaster, but it also reveals that how shared information is turned into knowledge and granted power is tightly bound to personal relations.

To try to address these variations in information sharing practices as they work across organisations and borders, disaster responders are increasingly engaging with sophisticated information systems to share information and enable inter-organisational collaboration (Harvard Humanitarian Initiative, 2011). One range of these technologies includes cloud-based warehouses that compile data from a variety of globally scattered emergency response agencies that can be searched as needed for information regarding a type of disaster. They store everything from community phone calls providing specific, local details to general disaster plans and lessons learnt that enable one response agency to learn from the activities of another. As they gather and make data shareable, these technologies are intended to encourage among their users shared understandings, respect, and greater ability to work together. In other words, the idea is that by using these disaster information technologies, not only will disaster planners and responders be better prepared because they have a wider breadth of information available, they will also build stronger communities, both among disaster responders and the publics that they serve.

Because these technologies have the ability to track sources and users, they are increasingly developed with an on-going focus on privacy and anonymity preserving techniques; techniques that are partly mandated by EU law. What is required of these techniques stands at the intersection of law, ethics, and organisational practices; an intersection that offers no clear directions or delimitations.

Anonymity, disasters, and exceptions to the rules

At its most basic level, anonymity is achieved when those seeking information cannot link specific data back to any identifying features of an individual. Colloquially, anonymity is treated as a Boolean status: personal details are either linkable to you or they are not. For example, Pfitzmann and Kohntopp (2001) describe anonymity as the state of an individual to be identified within a set of subjects. Legally, anonymity as a practice is intended to protect privacy. Privacy is

similar to anonymity in that it keeps identifying features from being shared. But whereas for privacy those features exist somewhere in an information system but are just not made shareable, for anonymity they do not exist anywhere. Nevertheless, the main purpose of both concepts is to act as forms of personal protection. They both offer individuals safety when there is the potential that threats to the person could occur if they can be identified. Doing so provides a strong basis for a secure public civic society where individuals do not feel at risk and thus can participate as needed in public life. However, in practice, such definitions are neither easy to evaluate nor easy to codify. Claims to anonymity are always relational, as they are defined in relation to national security and the protection of the common good (Nelson, 2011).

Moreover, as more information is linked together, EU law has had to define a new category: pseudonymity. Pseudonymity, as a legal concept, acknowledges that though data might be anonymous in isolation (e.g personal identifiable features not linked to stored data), once this data is integrated and analysed with other data sets, patterns could emerge that make it possible to link back to the person in new ways. Recent EU Data Protection Regulation (EU Regulation 2016/679) has had to include this legal concept of pseudonymity, now defining anonymity as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information' (Article 4 (5)). Anonymity can be lost if anonymous data is combined together and it is up to the responsible party controlling that data to determine when such risks might be necessary and accountable (EU Directive 95/46/EC). And combining data together is exactly what happens during disaster information sharing.

By engaging with practices of anonymity, individuals are implicitly articulating relationships between identity, personal responsibility, political community, vulnerability and social authority (Hansen and Nissembaum, 2009). Anonymity can relieve fear of persecution. The un-linkability of information to a person has the potential to provide a form of authority where socio-political power is otherwise lacking (North, 2003). For example, if a person providing information during a crisis could be identified by a hostile organisation, not only would the source be put at risk for prejudice and recrimination, but it would also likely mean they withhold information that could strengthen their community's safety and recovery (Burns and Shanley, 2013). How that work is done matters not only to individual safety but also to how communities interact and find value in each other's actions.

These complex interrelations between aim, definition, relativity, and value of anonymity as a practice are very visible in the difficulty the EU has in defining regulations around anonymity and related privacy issues. To determine what is a reasonable attempt at providing anonymity, the law states, 'account should be

taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments' (EU Regulation 2016/679: Recital 26). What counts as these objective factors is situationally dependent: the amount of money and time needed to create and use algorithms to run a specific data set using a specific technology. Moreover, according to the EU Data Protection Regulation, it is lawful to process personal data – without consent – if it is necessary 'to protect the vital interests of the data subject or of another natural person' or 'for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (EU Regulation 2016/679: Article 6 (d and e)). If it would help someone else or for a greater good, then a person's anonymity can be legally compromised. In other words, whether something is considered legally acceptably anonymous is not about a specific, clearly defined de-linked state. It is about whether the practice of linking or delinking is worth the effort to the parties involved or worth something to society.

Part of the difficulty of a clear and clean definition in this area is that legal mechanisms to protect humanitarians within international law, both customary and codified, derive from regulations concerning armed conflict, war, and criminal acts (Fast, 2014). This derivation builds into it an 'exceptional' approach to disaster management. One reason for this need is built into the causal nature of disasters: if disasters could be pre-defined in their entirety such that rules could be established, they would be mostly preventable. But, of course, they are not. While disasters emerge within the structures of society, they also occur because of what is made invisible within the norms of society (Davis, 1995; Hilgartner, 2007). Disasters are not exceptions to the norm; they are exceptions to expectations and understandings enabled by the norms.

As such, disasters justify making exceptions to the rules. They carry with them belief that efficiently achieving response goals, following the spirit of the regulations, and meeting social expectations are of greater value than the letter of the law (Zack, 2009). Similarly, legal exceptions include processing personal data without consent for 'humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters' (EU Regulation 2016/679: Recital 46). Consequently, when faced with disaster, having the necessary information and technology that can temporarily allow exceptional data processing to make decisions about the situation can be more acceptable, and even more legally permissible, than the regulatory 'status' of the data used (Jasmontaite, 2016). The transgressions are not just excusable but necessary for social cohesion and resilience. But these decisions have the ability to shift the normative rules that

structure power relations, inclusion, and exclusion (Ignatieff, 2005; Sandin and Wester, 2009).

The complexity of what it means to practice anonymity demonstrates the tension between notions of security and considerations of human rights, especially when different countries adopt different stances, even within the EU (Scheppele, 2006), or when trying to synthesize emergency power and liberal democracy (Scheuerman, 2006). Ultimately, anonymity is bound to the situation of information searching; to the who, when, what, and medium of information sharing. It is grounded not just in the capacity for physical links but also practical and political concerns like resource expenditures necessary to make those links. As highlighted by Nissenbaum (1999), these tensions are inherent in the interaction between new technologies and anonymity: it is all a matter of degree and layering.

In the uncertainty and unpredictability brought by disasters, this situational value judgement is a point of contention for emergency responders, as they try to manage their responsibility towards their communities and determine what kind of personal data practices can best produce community resilience (Li and Goodchild, 2010). Is this produced through privacy or non-discrimination? How much needs to be known, or not known, about an individual to ensure non-discrimination? Disaster information managers have to address individual needs while also considering the larger social context. They have to support community building but also build figurative firewalls that provide security to those within their bounds. As the solutions to these problems change from one situation to the next, so too does the understanding of what it is that anonymity is, what it provides, and what it protects. Exploring how anonymity is practised in engagements with disaster IT systems can help deepen the understanding of the intricate relationships between vulnerability, community, protection, and authority.

Building disaster management around anonymous sources

These many interoperable uncertainties faced by disaster responders in the EU have led to an EU-wide commonplace practice of providing a grade to information. This grade represents both the accuracy and the importance of the information coming in. Grading can help responders determine how urgent the situation is, what kind of corroboration is needed, how quickly an issue will disrupt the basic functions of a given society, and what kinds of actions to take. Even more, this type of determination can help responders know when they can and should make exceptions in how they engage with the data. If information is graded as highly urgent and as potentially impacting a large part of a society, then it is easier for disaster responders to justify the need to work in the legally flexible framework of

exceptions. How the practitioners define these grades is directly tied to the ability to identify their sources. However, if data is valued more when the source is known, what happens to urgent anonymous data?

Knowing who provided the information matters in relation to how quickly the information becomes valued. Such knowledge can increase the level of importance and urgency of the information provided (Bannon and Bødker, 1997). This is true for a Senior Liaison Officer for a UK Hazardous Area Response Team, who has undergone special training to gather and share information between agencies engaging in search and rescue or tactical medical operations during hazardous situations like toxic chemical leaks, collapsed buildings, or explosions, who stated: 'the more information you have from the key decision makers, the quicker you can resolve the incident and return to the new normality' (Hazardous Area Response Team Liaison, UK in April 2015). This is also true for a member of the UK ambulance service that responds by sending out paramedics to emergency medical calls throughout a region, who stated in this exchange:

> Q: How do you know your data is reliable?
>
> A: Quality assure it? Generally where the data has come from. Have to get to know the people - because what may be a cardiac arrest for one person is a minor scratch to another.

If there is no history with or of the author of the information, then the information is likely to remain low on a list of things to deal with. While providing data anonymously can protect against a range of surveillance issues and support necessary risk-taking, it can also limit the production of shared-meaning. The integration of personal information with civil interactions is necessary in order to participate in a community (Nelson, 2011). This is partly because identity carries with it a history of engagements that form the foundation of social dealings (Fine, 2012).

But the problem is that not all information comes from these identifiable key persons. Sometimes it just comes from a local citizen or from a member of another agency who has never had any interaction with these services before. This data is very difficult to grade. A UK Police Chief who, during disasters deals with protection of life and property and preserving peace, stated that it is very difficult to provide grades because:

> People want to ring in anonymously, write in anonymously or e-mail anonymously as much as you can do. But this information comes in and if it's anonymous it is very difficult to follow up on, but you've got to keep it on file to think well it might be part of a bigger picture and then it does take time. I don't know what the answer

> is to that. People will either trust us or not, or trust other people or not. (Police Chief, UK in May 2015)

The police chief continued: 'you can keep people safe and anonymous, or you could feed the information in and that's how it's graded appropriately'. Anonymity could provide protection and security to vulnerable individuals by limiting who can access their identity or the situations in which it can be revealed (Puzar et al., 2008). But, the assumption behind the latter is that it keeps the source and the disaster responder at low risk and low liability for their actions, as it follows proper protocol and support formal decision-making. But this takes time, which could lead to larger community-based risks due to the inactions on the information as it worked its way through the grading protocols.

Information provided by anonymous sources goes into a data warehouse and waits, often unused, until there is more information to back up the concern or more information to provide context to help balance the lack of details about the source. The grade will change when multiple reports start to be connected together, such as when more than one anonymous persons report the same issue of concern or more than one information system is connected together that each contain a similar report. But this solution relies on some assumptions: all the information reaches the same place in a timely manner, such as the same warehouse; all the information is comparable with little effort in terms of time and money since otherwise the links that produce value will not be made; and that these acts of combining data will not produce situations of pseudonymity, in which anonymous individuals can be identified as a result of the interconnection of the various data points.

Even if personal data about the source is connected to the information within different agency databases, each agency has strict privacy rules that do not allow personal data sharing for the safety of the people they serve. If an issue is reported four different times, by four different anonymous reporters, to four different systems – taking full advantage of the different social organisations intended to support best social practices around risks and disasters – then the information will likely remain as invisible as if it had been provided anonymously unless there is a system put in place in advance. However this is difficult to fully map out in advance considering the unexpected nature of disasters. The situation gets even more complicated when the data has to cross borders, since as crisis and related personal data flows across national borders, it faces different data protection regulations as well as limitations on what and how that data can move across a new boundary, creating barriers in the sharing of critical information (Burns and Shanley, 2013). Anonymity here is less about de-linking data from person and is more relative to privilege for accessing data and resources for managing legal protocol.

The invisibility provided by acts of anonymity produces a social security when participating in political life data (Nelson, 2011; Secor, 2004). The need for security is unavoidable when dealing with the management of cultural differences, especially contentious ones, like in cases where religion is involved. Being unidentifiable or untraceable provides safety for individuals and their related communities at times of political opposition or transgression. This can be important when claims of favouritism are floating about, as often is the case in disaster aid, or when one group is facing persecution because they have some connecting characteristic with those more directly involved in a disaster. Or when there is a lack of trust in formal response and anonymity leads to sharing of information that does not follow the traditional and more formal lines of disaster management (Rizza et al., 2013; Starbird et al, 2015).

The answer to how the information is sourced, however, is vital to a responder's ability to do their job and mitigate risks. For instance, police in the UK have to manage their interactions with the public carefully, including data provided by members of the public, as their powers are only as strong as public consent. If the public does not trust or think that data is being handled properly or transparently, then that consent could be limited or even withdrawn. Anonymity becomes a tool directly related to trust: trust, or lack thereof, of the source in the safety being provided by the disaster responder; and trust, or lack thereof, of the responders in the validity of the source.

But, while anonymity can protect an individual from the feared harm that might come from identifying oneself and can make data interoperable between systems, it can also erase a category of need or the nuanced socio-cultural differences that could suggest a different pattern of disaster planning and response. As information is shared via IT systems, the necessary socio-technical practices of making information interoperable and comparable ends up abstracting individuals (as sources and within information) to match the bureaucratic needs in order to support interoperability in disaster management (Paganoni, 2012). Within such generalities that make interoperability possible, differences in definitions of need, aid, recovery, and support are often missed by the governmental disaster responses that have to manage many diverse communities at once (Henderson, 2011). Doing so walks a fine line between protection and obscurity, and masks differences that are integral to disaster responders who address diverse community needs, even as it supports a kind of sharing information that makes it possible for different responders to work together.

Being anonymous can lead to the invisibility of unique needs and differences becoming the norm. This norm, as expressed in our interviews, can be an expectation that as a source an individual can, and thus should, be anonymous. It

was also expressed as an expectation that anonymity anticipates discrimination, thus reinforcing that discrimination as the norm. As a result, without critical, situational engagement, anonymity can reproduce the difference and exclusion that required anonymity in the first place (Carlson, 2011). These practices have the potential to act as an exclusionary, instead of a protective, force for diversity.

In such cases, despite lowering the local risk to an individual, anonymity can put communities at risk because of how the action derives from the gaps left in place by the anonymity. In other words, anonymity erases the social relations that build trust, and thus more work has to happen before there is enough trust to know how to engage with the anonymously provided information, and, vice versa, more work has to happen before the sources providing the information have enough trust to not request anonymity. If the gap is too large, then the procedure is to hold, wait, and risk inaction.

Building communities of action around anonymised social and organisational relationships

Emergency responders use their daily contacts at work to develop relationships, internal and external to their organisation, that help them accomplish their goals. The people encountered on-the-job become confidants, fellow experts, trusted sources for off-the-record discussions to support the necessary information analysis:

> It's about trust, I suppose. By getting to know the people so you know what you need to do automatically, so they don't have to ask, so you just share for their benefit. (Senior Fire Officer, Ireland in April 2015)

These interactions make it possible for one practitioner who has information they know should not be shared to find creative ways to share what is vital about it without directly breaking the rules. For example, when a medical professional refers to a victim injured during the chaos of a disaster who is known to have a contagious blood disease – personal medical information that cannot be shared with other responders – the medical professional can say to their colleagues: 'I would use gloves with this individual' without directly breaking the privacy laws. Or, when speed matters, these people are already contacts that exist in one's personal mobile phone, making a call a quick and easily identifiable tap away instead of relying only on the more formal practice of putting the information into the digital information systems to be found. When discussing why such blurry, semi-exceptional interactions were needed, many of those interviewed expressed similar statements as the one below:

> It might take a bit of time to get through the process in which time that individual who is drink driving may have had an accident and injured someone else. So you have to make a personal call sometimes and say that needs dealing with right now. (Police Chief, UK in May 2005)

But these information channels are not just about sharing data under-the-table for the sake of simplicity. These personal connections that make up these communication pathways support the responders as they find themselves in positions of making individual decisions about the data they encounter. In such situations, the authority to determine what data they should and should not see – and as importantly why – is not in the hands of the state or even their agencies, but in their individual hands because of the urgency of the situation.

The informal and personal connections provide not only a level of trust, but also a level of leeway because knowing with whom you are working removes much of the fear of liability of an error in information sharing. For example, when asked if this tendency to share with greater value on speed than procedure during disaster situations ever led to getting personal data he did not think he should have, one responder replied:

> Maybe at times, but you don't dwell on it, use the bit you want and keep going. It's not like you go 'oh I found something juicy here that I shouldn't know about'. (Senior Fire Officer, Ireland in April 2015)

Despite getting his hands on information that should have been anonymised, because he knew who he got it from and understood the context in which it was being shared – particularly the urgency of the sharing – the responder did his best to rebuild the anonymity in his informational gaze and neither were concerned about liability.

The same flexibility and trust does not appear when dealing with information from a generic role in disaster management instead of the individual in that role; a colleague in another agency with whom one actor has a history will be trusted faster than just any old police chief that does not have a face but is defined by their role. Typically, judgements about the legal leeway in data protection and protocol are grounded in situational details and urgency that do not make it into final incident reports. However, as data sharing is carried out in a technological environment that does not have the same situational grounding, fear of technological surveillance and related liabilities will often impede any sharing that is not cleanly on the side of data protection.

Designers are struggling to design disaster IT in a way that can collect data about a source that supports the most efficient and trusted information sharing practices, but in a way that does not turn organisational decisions into situations of

individual liability. A UK Senior Civil Contingencies Officer described it like this: if there are records of a specific firefighter making the ethically and legally challenging decision of letting one house burn in order to save ten others then suddenly that individual becomes liable for his actions. Instead, if the report goes into a data system as belonging to an agency or a role, anonymising the individual making the decision means that the liability goes back to the organisational level. However, doing so limits the ability to work in the framework of personal relations that form such a strong basis for disaster response work and weakens the community built as responders share and act upon information jointly.

Trust in the source of information is vital for full participation within a community (Allen, 2007). If a responder does not trust who they are receiving their data from, they will neither engage with the data nor act in solidarity with that actor's organisation. Consequently, setting the framework for trust is the basis for how requests are often made for information, especially information that might fall on blurred legal lines. As explained by an emergency legal expert from Germany who helps manage the laws around anonymity and data protection:

> We try to give reasons for all the data we want to have. We want to explain why we need this data. And we hope if we explain why we need this data we will get it...We have to discuss often the willingness of the persons to whom these data belong. (Legal Expert BBK, Germany in June 2015)

These engagements are based around providing the answers before the questions arise, to encourage the type of inclusion needed to build not just trust, but also a community of active, equal, participants. For instance, the emergency legal expert above hopes that the explanations can provide an equivalent to this personal history, both of the responders' own needs, but also of the individuals or situations about whom they are seeking data. Without such history, it is much harder to legitimise future interactions, or to act in solidarity. This need also signals a lack of openness; a fear and a sense of a need for protection, reinforcing those power structures that require anonymity (Secor, 2004).

Anonymity, here, acts to protect a specific form of participation in a specific set of power structures. As part of digitally shared information, anonymity formally limits liability, but still makes space for the face-to-face social connections that allow for information to be shared directly from person to person in ways that are not easily classified or categorised but still legally permissible. In doing so, practices of anonymity can create situations where not everyone has equal access to such practices (Garber, 2000), such as when new forms of response emerge, like crisis-mapping. Such cases require the inclusion of new actors in the response that do not have the same cultural or political histories with data sharing. This unequal access to practices of anonymity affects not just how individuals are

protected through data de-linking, but affect how a disaster becomes known and acted upon.

As a result, anonymity often becomes a tool of unintentional power, playing a role in defining who has the right to define what a disaster is and how a disaster is responded to. But doing so can also close off opportunities for cooperation (Garber, 2000). Anonymity keeps relations between individuals and organisations as they were, reinforcing current power structures, emphasising divisions, and raising questions about who should be trusted.

Conclusion

Here is one of the fundamental challenges being faced in information sharing for disaster management. On the one hand, information is being digitally collated across systems in a way that is safe and secure and protects the data and the individuals represented by the data (as source or subject). This collation is being done via classification schemes to help make the data more visible and interoperable in order to continue to provide the authors of that data the right to be anonymous while also giving them a place in society. On the other hand, information is often dealt with through personal experience and informal pathways, from one person to another, in order to make sure a concern gets addressed. While this might mean less exception on the small scale (e.g. one responder picking up the phone for an off-the-record talk to help with sharing and risk analysis), it can also mean more exception on the wide scale in order to get past the limitations of the protocol, legal language, and technological codified information. As a result, anonymity produces community and connects to organisational power structures in two different, competing, ways that stand at the intersection of protection and discipline.

Anonymity is enacted to help support equal protection among those being served by the disaster responders. It is enacted as part of civil community practices that support shared meaning and equality, and opens up possibilities for negotiating difference and protection without prejudice or discrimination. It can level the playing field providing opportunities for all actors involved – responders and the affected individuals and communities – to find value in each other's actions. In the case of the former, anonymity can protect those who fear liability for decisions they make in the urgency of the moment, where being visible can keep actors from making risky, but potentially life-saving, decisions. In the case of the latter, both individual actors or entire communities that, prior to the disaster, were marginalised by socio-political relations, can use disasters as an opportunity to work to gain a new voice in both the larger organisation of disaster response, and potentially society as a whole (Palen and Liu, 2007).

But, relying on anonymity as a solution can hinder solidarity and limit openness to changes in disaster management practices. Disaster organisations are built upon networks that require history of engagements for best practices and a level of organisational trust. Speed of decisions and actions are connected to identity, while working around systems grounded in anonymity becomes a necessary means to bring the different organisations together. The added work that is necessary to balance the anonymously sourced information with information that comes from key, and trusted sources, can put the same communities seeking protection at risk. Making data interoperable between systems often requires generalisations that discipline actors and problems into specific understandings, masking cultural and political differences that are vital to disaster response. Anonymity becomes a tool of unintentional power, shaping who has the right to define not only how a disaster – and response - unfolds but how the disaster is understood to put people at risk in the first place.

These two layers of anonymity practices – simultaneously producing and hindering solidarity, community, and organisational change – intertwine in the information exchanges around disasters. They emerge from the socio-technical acts intended to support participation in the type of civil interactions and community building required by disaster. What should be codified in law and technology is not just the state of the data as personal data or de-linked data. The focus needs to be on the work anonymity does and its connection to the protection both of the rights of individuals *and* that of civil society. The focus should be on the role of anonymity in relation to the possibility of a shared meaning necessary for sensitivity to the multicultural and often tense political situations made visible by disasters. To understand how anonymity fits within these structures of disaster response, we need a better understanding of how anonymity can benefit and disadvantage individuals, communities, and publics in general. It needs to focus on how the official government response has to interface with ad-hoc community reactions, and how standard procedures have to relate to locally improvised solutions. There is also a need to evaluate how anonymity can support the maintenance of a cultural authority without costing another group its voice in order to encourage the development of a more nuanced understanding and acceptance of different community needs and more interoperable disaster IT.

Anonymity, as a concept, does not automatically engender inclusion or exclusion. Instead, data and privacy structures need to acknowledge the disaster specific social and technical forms of organising to see how new norms around protection and discipline might emerge. How anonymity works within social organisation and technological structures needs to be considered in the design and use of IT for disasters so that communities in need of aid do not experience exclusion or fear. The ability to provide data anonymously can provide an opportunity for

communities that have not had a strong voice to speak more freely and equally, and allow those in ethically challenging positions to make necessary and hard decisions for their community without facing personal liability. But doing so also lessens the value of the information provided and the ability to understand the nuanced differences that make up a given society. Without such considerations, instead of having their needs supported and protected by the possibility of anonymity, already marginalised communities can have those political relations further reinforced by these systems. In the end, the value and role of anonymity in the community of disaster response depends on the questions being asked and the situation of asking.

references

Allen, B. (2007) 'Environmental justice and expert knowledge in the wake of a disaster', *Social Studies of Science*, 37(1): 103-110.

Bannon, L. and S. Bødker (1997) 'Constructing common information spaces', in J. Hughes, et al. (eds.) *Proceedings of the fifth European conference on computer supported cooperative work*. Netherlands: Kluwer Academic Publishers.

Burns, R. and L. Shanley (2013) *Connecting grassroots to government for disaster management: Workshop summary*. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars. [http://www.wilsoncenter.org/publication/connecting-grassroots-to-government-for-disaster-management]

Carlson, M. (2011) 'Rethinking anonymity: Problems and solutions', in *On the condition of anonymity: Unnamed sources and the battle for journalism*. Chicago: University of Illinois Press.

Davis, M. (1995) 'Los Angeles after the storm: The dialectic of ordinary disaster', *Antipode*, 27(3): 221-241.

EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281/31. [http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046]

EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L 119/1. [http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf]

Fast, L. (2014) 'Coping with danger: Paradigms of humanitarian security management', in *Aid in danger: The perils and promise of humanitarianism*. Philadelphia: University of Pennsylvania Press.

Fine, G. A. (2012) 'Action and its publics', in *Tiny publics: A theory of group action and culture*. New York: Russell Sage Foundation.

Frickel, S. (2008) 'On missing New Orleans: Lost knowledge and knowledge gaps in an urban hazardscape', *Environmental History*, 13(4): 643-650 .

Garber, J. (2000) 'Not named or identified: Politics and the search for anonymity in the city', in K. Miranne and A. Young (eds.), *Gendering the city: Women, boundaries and visions of urban life*. Lanham: Rowman and Littlefield Publishers.

Harvard Humanitarian Initiative (2011) *Disaster relief 2.0: The future of information sharing in humanitarian emergencies*. Washington, D.C. and Berkshire, UK: UN Foundation and Vodafone Foundation Technology Partnership

Hansen, L. and H. Nissembaum (2009) 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, 53(4): 1155-1175.

Henderson, K. (2011) 'Mind maps, memory and relocation after Hurricane Katrina', in R. Dowty and B. Allen (eds.) *Dynamics of disaster: Lessons on risk, response, and recovery*. New York: Earthscan.

Hilgartner, S. (2007) 'Overflow and containment in the aftermath of disaster', *Social Studies of Science* 37(1): 153-158.

Ignatieff, M. (2005) *The lesser evil*. Edinburgh: Edinburgh University Press.

Jasmontaite, L. (2016) 'Finding the legitimate ground for the processing of personal data of affected persons: First responders face uncertainty', *Journal of Contingencies and Crisis Management*, Forthcoming.

Klinenberg, E. (2002) *Heat wave: A social autopsy of disaster in Chicago*. Chicago: University of Chicago Press.

Li, L. and M. Goodchild (2010) 'The role of social networks in emergency management: A research agenda', *International Journal of Information Systems for Crisis Response and Management*, 2(4): 49–59.

Nelson, L. (2011) 'Anonymity', in *America identified: Biometric technology and society*. Cambridge, MA: The MIT Press.

North, M. (2003) *Anonymous renaissance*. Chicago: University of Chicago Press.

Nissenbaum, H. (1999) 'The meaning of anonymity in an information age', *The Information Society*, 15(2) 141-144.
[http://www.nyu.edu/projects/nissenbaum/paper_anonimity.html]

Oliver-Smith, A. (2002) 'Theorizing disaster: Nature, power, and culture', in S. Hoffman and A. Oliver-Smith (eds.) *Catastrophe & culture: The anthropology of disaster* (23–48). Santa Fe: School of American Research Press.

Paganoni, M. C. (2012) 'City branding and social inclusion in the global city', *Mobilities*, 7(1): 13-31.

Palen, L. and S. Liu (2007) 'Citizen communication in crisis: Anticipating a future of ICT-supported participation', *Proceedings of CHI 2007*: 727-736.

Pfitzmann, A. and M. Kohntopp (2001) 'Anonymity, unobservability, and pseudonymity – A proposal for terminology', in H. Federrath (ed.) *Designing privacy enhancing technologies*. Berlin: Springer-Verlag.

Puzar, M., T. Plagemann and Y. Roudier (2008) 'Security and privacy issues in middleware for emergency and rescue applications', *2008 Second International Conference on Pervasive Computing Technologies for Healthcare*. IEEE: 89-92.

Rizza, C., A. Pereira and P. Curvelo (2013) '"Do-it-yourself justice": considerations of social media use in a crisis situation: The case of the 2011 Vancouver riots', *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany*: 411-415.

Sandin, P. and M. Wester (2009) 'The moral black hole', *Ethical theory and moral practice*, 12(3): 291–301.

Scheppele, K. L. (2006) 'North American emergencies: The use of emergency powers in Canada and the United States', *International Journal of Constitutional Law*, *4*: 213–43.

Scheuerman, W. E. (2006) 'Survey article: Emergency powers and the rule of law after 9/11', *Journal of Political Philosophy*, *14*(1): 61–84.

Secor, A. (2004) '"There is an Istanbul that belongs to me": Citizenship, space, and identity in the city', *Annals of the Association of American Geographers*, 94(2): 352-368.

Starbird, K., D. Dailey, W. Hayward, L. Ann, M. Thomas, R. Pavia and A. Bostrom (2015) 'Social media, public participation, and the 2010 BP Deepwater Horizon oil spill', *Human and Ecological Risk Assessment: An International Journal*, 21(3): 605-630.

Zack, N. (2009) *Ethics for disaster*. Lanham, Md.: Rowman and Littlefield Publishers.

the author

Katrina Petersen is Research Associate at the Centre for Mobilities Research, Lancaster University. She works on the SecInCoRe project, concerned with the design of secure

dynamic cloud concept for crisis management based on a pan-European disaster inventory. She focuses on the collaborative production of visual representations, data sets, and information technology that form the basis for sharing information between diverse and distributed actors during disasters. Her background is in science and technology studies, communication studies, public engagement in science museums, and geology.
Email: k.petersen@lancaster.ac.uk

Monika Büscher is Professor of Sociology at Lancaster University, Director of the Centre for Mobilities Research (Cemore) and Associate Director at the Institute for Social Futures. Her research explores the digital dimension of contemporary 'mobile lives' with a focus on IT ethics and the informationalisation of risk governance, with national and international projects (BRIDGE, SecInCoRe). She holds an honorary doctorate for her work in participatory design from Roskilde University. She edits the book series Changing Mobilities (Routledge) with Peter Adey.
Email: m.buscher@lancaster.ac.uk

Catherine Easton is Senior Lecturer in Law at Lancaster University. Dr Easton's research interests focus upon internet governance, domain name regulation, intellectual property, access to technology and human/computer interaction. She also carries out research on teaching law with technology. She is on the steering committee of the UN's Internet Rights and Principles coalition.
Email: c.easton@lancaster.ac.uk