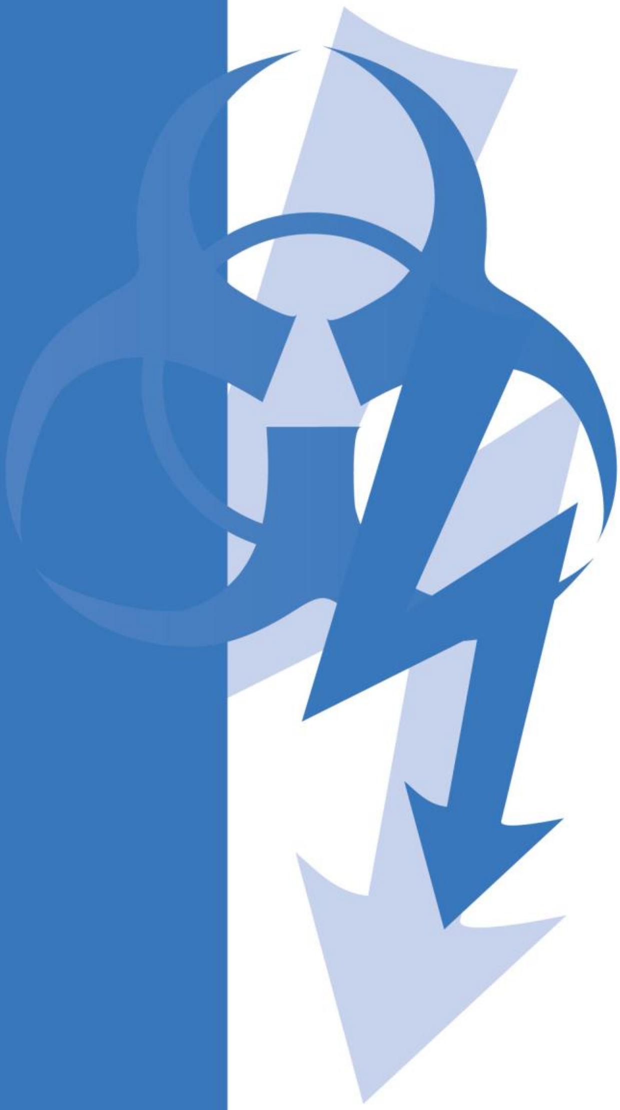
centre for analysis
of risk and regulation



Making sense of inter-organizational ‘safe spaces’ in business regulation

Julien Etienne

DISCUSSION PAPER NO: **79**
DATE: **October 2015**

THE LONDON SCHOOL
OF ECONOMICS AND
POLITICAL SCIENCE

Making sense of inter-organizational 'safe spaces' in business regulation

Julien Etienne

Contents

Published by the Centre for Analysis of Risk and Regulation at the
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
UK

ISSN 2049-2718

Making sense of inter-organizational ‘safe spaces’ in business regulation

Julien Etienne

Abstract

For regulators, gathering information about the activities they regulate is crucial. For businesses, sharing information across can help address common issues better. Yet, businesses would generally not willingly share sensitive information with regulators or competitors. To overcome such reluctance, one may set up forums or channels of communication within which businesses would feel protected enough to share information with peers and regulators. Such ‘safe spaces’ have been discussed frequently, sometimes put in place, but rarely studied. To address this gap, this article presents a study of incident data sharing in the chemical and oil industries in France and the United Kingdom. It identifies multiple obstacles for information sharing that safe spaces would have great difficulty addressing. Hence, safe spaces would generally be fragile, contested, and poorly institutionalized. One should not overestimate their ability to deliver information to regulators, or to achieve self-regulation in an industry.

Introduction

To fulfil their mandate, business regulators need to gather information that only businesses possess (Vaughan 1990). For instance, regulators may need information on the nature of business activities, the technologies used and how they evolve, so that they may elaborate or revise regulations accordingly. Regulators may also need information on business practices, particularly those that contravene the spirit or the letter of regulations, so that an appropriate response may be brought to them.

Previous studies have shown that business regulators would often struggle in their efforts to 'close the information asymmetry gap' between them and the businesses they regulate (Macher et al. 2011; also Beaumont 1979; Etienne 2015; Vaughan 1990). Nowadays, they often lack the capacity or the authority to appropriately monitor the ever growing complexity and global character of business organizations and supply chains. Besides, financial resources that could fund state-led information gathering efforts have been drying up in many countries in the post-financial crisis years.

Alternatively, regulators may also rely on others for providing information. Thus, individuals (generally, employees) who would have direct knowledge of mishaps, or misconduct may report them to regulators (e.g. Dekker and Laursen 2007; Mills 2013; Reason 1997). Alternatively, business organizations may also voluntarily share information, which is the topic of this paper.

Arguably, enhanced information flows between businesses and regulators not only contribute to regulatory effectiveness (e.g. Mills and Reiss 2014); they might also fuel a process of industry self-regulation, with regulators only taking a secondary role (e.g. Gunningham and Rees 1997; Rees 1997). Yet, achieving genuine business reporting to other businesses and regulators is a difficult endeavour. Indeed, to see businesses actively sharing with others information that could be damaging to them is unlikely: there are risks involved for the sharer. That is particularly the case if those organizations receiving the information are competitors or enforcers. Depending on the information shared and the environment they live in, sharing organizations may suffer reputational damage; they could face legal consequences; or they could suffer from unfair competitive practices. Thus, organization scholars have long argued that secrecy is a default response from organizations to their environment's demands (Pfeffer and Salancik 1978).

Aware of those risks for business organizations, a number of regulators and industry stakeholders have considered setting up so-called 'safe spaces'. Safe spaces can be understood as *forums or channels of communication set to shield business organizations from the risks of sharing potentially sensitive information with their peers and/or with regulators*. For instance, in the aftermath of the horsemeat scandal (a large-scale fraud affecting the market for red meat in Europe), the Elliott Review in the UK called for the setting up of a 'safe haven' to enable intelligence on possible fraud to flow better from industry to regulators:

> Industry is very keen to work with regulators, but is cautious about the legal implications of providing information and intelligence unless information has previously been anonymised from any direct attribution to a particular source. This flow of intelligence from industry to Government is a vital part of the systems that must be developed. … Given the concerns about sharing even sanitised information with regulators, industry will need further reassurances. The industry must ensure that all those with an interest, including key trade associations, as well as SMEs, are involved in developing the 'safe haven' and that it is set up as soon as possible.
>
> (Elliott 2014: 26–7)

Although frequently entertained by practitioners, the notion of inter-organizational safe space is not a clear or settled concept, nor a well understood phenomenon. This reflects the lack of scholarly work (empirical or theoretical) on the topic, in contrast with the literature on intra-organizational processes of information gathering and reporting, which is substantial (e.g. Feldman and Lobel 2011). Besides, the dynamics of inter-organizational safe spaces could not be easily inferred from knowledge on intra-organizational safe spaces, since organizations are certainly different from individuals and cannot be assumed to behave as they do. Accordingly, whether inter-organizational safe spaces 'work' at all is also far from clear.

Our poor understanding of safe spaces may also reflect the extensive empirical variations one may observe in the field. Safe spaces come in many shapes, can be found in a wide variety of sectors, are set up to address varying issues (such as safety, fraud or sustainability), and may operate in highly variable ways. Thus, while some appear to function primarily for the benefit of regulators, others function for the benefit of industry, and others for both.

Some of these spaces are meetings where participants discuss issues face to face. This is the case for 'Responsible Care Cells' (see below), through which representatives of chemical industry firms meet at regional level, sometimes in the presence of regulators. But other safe spaces may operate via intermediaries, acting as relays and buffers between participants, and may include only firms or regulators as well. For instance, the 'safe haven' mentioned above relies on a third party to collect, sanitize, and re-distribute intelligence, without any face to face interaction between participants.

The type of information exchanged within safe spaces may also vary considerably from one to the next. In principle, some safe spaces exist to facilitate the exchange of information on participants' failures (Responsible Care cells host discussions on incidents). In others, participants are deemed to exchange best practice information. For example, participants to the Food Ethics Council meetings in the UK have discussed how they manage the environmental impact of their practices. Others (e.g. the safe havens called for in the aftermath of the horsemeat scandal, including the UK) are meant for exchanging information on other firms, particularly suppliers, and notably what sampling tests might have revealed about the quality of those supplies (suggesting fraud). On top of all that, participants in safe spaces might actually drift from the safe space's mandate and share other types of information than they are meant to. Indeed, unless very carefully managed by a strong, perhaps even an authoritarian lead, safe spaces are conducive to uncontrolled conversations that might drift in multiple directions.

This paper aims to begin filling up this knowledge gap on a topic that is of great interest to many business regulators worldwide, but has received very little scholarly attention to date. The main goal here is to better outline the key features of safe spaces and thus begin to understand how they do or do not work. On that basis, the paper aims also to outline a few elements for a theory of safe spaces. It approaches safe spaces from the ground up, and cross-nationally. It presents empirical data on efforts developed by regulators and industry bodies to improve information sharing on incidents in the chemical and onshore oil industries in France and the UK. It explores the dynamics at play leading to more or less sharing of sensitive information between businesses, and between business and regulator.

The paper's findings point towards multiple obstacles hindering safe spaces. Some of those obstacles are external, reflecting the inherent tensions between information sharing and the broad environment of firms and regulators. Indeed, when regulators or industry leaders support or contribute to safe spaces, they effectively have to negotiate their relationship to key principles and institutions, chiefly: the rule of law, market competition, and the public right to know. The outcomes of these negotiated arrangements may vary widely, as argued here, because of different institutional, cultural, economic, or political factors. Whichever the outcome, safe spaces are also constrained internally. Participant organizations, even if shielded from external pressures, are also bringing their mixed goals and demands to safe spaces, which may not be compatible with collective learning and the achievement of inter-organizational or societal interests. Some of those constraints may be mitigated (goals may be better aligned by ensuring that participants belong to a homogeneous group), but that may increase tensions in other respects (risks of excessively aggressive competition or anti-competitive collusion). In other words, safe spaces often appear severely and irremediably constrained. As a result, it is reasonable to assume that safe spaces will rarely become institutionalized, whether they operate for the purpose of gathering information for regulators, or to enable industry self-regulation. This puts them in stark contrast with safe spaces for individual reporters, which have been successfully institutionalized in many different organizations and a few industrial sectors.

In the next section, I summarize the relevant literature, outline my methodology and research design. The empirical material is organized around three key principles that have shaped safe spaces in conflicting ways: transparency, accountability, and competition. On the basis of the empirical material I then offer elements and suggestions towards a theory of 'safe spaces' in the discussion section.

Literature review

The academic literature explicitly addressing the idea of inter-organizational safe spaces in business regulation is sparse: Rees' study (1994) of the Institute of Nuclear Power Operations (INPO) is, to my knowledge, the only empirical study of an inter-organizational safe space published. In comparison there is abundant literature on 'safe' reporting systems for individual employees, most of which operate within business organizations. The socio-legal literature includes studies on how information is exchanged (or not) between regulators and regulated organizations, describing ways such encounters may be made 'safe'. In this section I rely on that extended literature to draw initial insights about inter-organizational safe spaces.

The notion that information might flow better if reporting it is made 'safe' is primarily anchored in the management / organization studies literature. James Reason has argued that individual reporting schemes are likely to work better if a few conditions are satisfied, notably: 'indemnity against disciplinary proceedings …; confidentiality or de-identification; the separation of the agency or department collecting and analysing the reports from those bodies with the authority to institute disciplinary proceedings and impose sanctions' (Reason 1997:197; also Dekker and Laursen 2007; Johnson 1996; Mills 2013). By contrast, a 'blaming' approach has been associated with poor information exchange, a lack of learning, and catastrophe (Chikudate 2009). From early on, this literature identified principles and mechanisms of transparency and accountability as potentially key obstacles to information flows within organizations.

These conclusions are echoed in regulation / socio-legal studies of information exchange between regulated firms and regulators. Exploring whether information could flow from regulated firms to regulators, contributors have emphasized how that may be hindered by the risks this entailed for the reporter (in the form of sanctioning, damaged reputation, and the likes). Accordingly, scholars have argued that self-reporting should be made safe, for example by granting immunity and/or anonymity to reporters (Innes 2001; Parker 2002; Stafford 2007). Similar ideas have informed the setting up of the Self-Audit programme run by the Environment Protection Agency in the United States (EPA 2000; Pfaff and Sanchirico 2004), protected self-reporting programmes run by the Occupational Safety and Health Administration (OSHA; Lobel 2005), and the Voluntary Disclosure Reporting Program (VDRP) set up by the Federal Aviation Administration (FAA; Mills and Reiss 2014). Companies enrolling into those programmes have been formally granted immunity or a more lenient treatment (i.e. reduced penalty) for self-reported failures or breaches.

Yet, empirical studies have questioned the effectiveness of making self-reporting by businesses 'safe'. Numerous authors have suggested that immunity rules have encouraged gaming behaviour, and generated partial and carefully managed information (see especially Helland 1998; Pfaff and Sanchirico 2004; Stafford 2007). This contrasts with studies of intra-organizational reporting, which have generally been quite positive about the impact of anonymity/immunity guarantees for individual reporters.

Joe Rees' study of the INPO (1994) has also provided a mixed picture of business reporting and secrecy. Rees' is the only thorough study of an inter-organizational 'safe space' published. The INPO was set up in the aftermath of the Three Miles Island accident as an industry-only forum. Away from the eyes and ears of external parties, including the regulator's, the INPO has collectively discussed the performance (good and bad) of its members. According to Rees, it has been a remarkably successful self-regulatory institution. However, Rees has disputed the argument that the INPO had to be 'safe' from external scrutiny in order to work effectively (Rees 1994: 118–20). Various other scholars and stakeholders have expressed similar doubts (ibid.: 188–89: n14, 214–15: n57). To Rees (1997), the fact that the INPO had effective authority over industry players and that the latter developed shared norms (an 'industrial morality'; Gunningham and Rees 1997) have been more important factors than secrecy for its institutionalization and effectiveness. Rees has speculated on a future in which the veil of secrecy at the INPO would be removed.

In Rees' trails, during the self-regulation fad, scholars have looked for other 'institutions' of industry self-regulation. Some have considered the chemical industry's 'Responsible Care' (RC) initiative a likely case. RC was set up by the industry in North America in the late 1980s and expanded worldwide in the following years. Among other things, RC has encouraged firms to participate at safety-themed meetings that exclude non-members (i.e. safe spaces). Arguably, RC developed at a time when the chemical industry's views on the environment were changing (Hoffman 1999). Sometimes, scholars have assumed from the existence of RC or similar industry initiatives, that it is an 'institution' performing an effective self-regulatory function. However, empirical studies have exposed this 'bad functionalism' (Barnett and King 2008) as contrary to the INPO, RC has had limited effectiveness (King and Lenox 2000; Prakash 2000; Rees 1997). The more recent assessments of RC have actually contributed to downplaying its role either as a 'safe space' for inter-organizational learning or as a self-regulatory initiative, and rather emphasized its function as a communicational and reputational tool (Barnett and King 2008).

In sum, very few scholars have discussed *inter*-organizational safe spaces and as a result these have remained an ambivalent and relatively misunderstood phenomenon. The literature emphasizes their role as shields against demands for transparency and accountability, arguing that these are key obstacles to information sharing. Yet, the only empirical study available (Rees's) has actually questioned the necessity for inter-organizational 'safe spaces' to be 'safe', with particular reference to the secrecy of INPO's operations. It has instead emphasized the necessity of an authoritative moderator and shared norms to achieve institutionalization and effective self-regulation. The socio-legal literature has also suggested that making spaces safe to increase exchanges of sensitive information *between* interested businesses and regulators might have had unintended and/or perverse effects. That contrasts with the literature on *intra*-organizational safe spaces, which has brought more positive conclusions overall (e.g. Reason 1997). Hence, one can legitimately question whether inter-organizational safe spaces are different, how they work in practice, and why they might not perform as well as intra-organizational ones.

In the following pages I intend to begin addressing these gaps by laying out which factors might be considered when trying to make sense of the shape, workings and outcomes of safe spaces.

Method

Research design

The evidence presented in here is drawn from the exploratory phase of a comparative study that looked at two countries: France and the United Kingdom. The fact that data is drawn from two instead of one country enables more nuance to the argument. Yet, that nuance does not amount to a clear enough contrast that could then be explained by making reference to differences between the two countries. Indeed, there is not enough data and evidence accessible to develop a controlled comparative design. In other words, in the absence of firm goalposts (for instance, on the level and detail of information reported), expanding the enquiry to these two countries enables increasing variability, and mitigates the risks of over-interpreting from a single case. Hence, this should not be read as a comparative study of two closely matched countries (the like of which is, for instance, discussed by Faure 1994). Rather, this is exploratory research, undertaken in the interest of drawing theoretical perspectives on a mostly unexplored topic (Gerring 2004). Accordingly, the approach is to explore the aims and meanings of inter-organizational safe spaces through the discourses of the participating actors. As we shall see, that approach sheds a nuanced light on the purposes and workings of safe spaces.

The data was collected during a three-year project on incident reporting (2010–2013). Various stakeholders were interviewed in France and the United Kingdom. They were safety managers in onshore oil and chemical sites, representatives of oil and chemical industry trade associations, senior civil servants who were or had been working in regulatory agencies competent for the supervision of those firms, and 'street-level' enforcement agents from the same said regulatory agencies. About 60 interviews most of which were recorded, were drawn upon for this paper. All interviewees were promised anonymity. I drew also from databases, legislation, company reports, trade union reports, trade association documents, minutes of meetings (including meetings within 'safe spaces'), and press articles.

The research encountered several kinds of spaces where information about incidents was being shared fairly frequently, and more or less extensively among businesses themselves, and between businesses and (sometimes) regulators. Trade associations hosted and moderated forums where sharing information on incidents was a recurrent item on the agenda. They were: in the UK, the Chemical Industries Association (CIA), the Chemical Business Association (CBA) and the United Kingdom Petroleum Industry Association (UKPIA); in France, the *Union des Industries Chimiques* (UIC), and the *Groupe d'Etude de Sécurité des Industries Pétrolières et Chimiques* (GESIP). In a minority of those safe spaces, regulatory agencies participated in meetings: in the UK, the Health and Safety Executive (HSE) was engaged in some Responsible Care cells run by the CIA; in France the *Inspection des Installations Classées* (IIC) sometimes lead meetings hosted in regional organizations, known as SPPPI or S3PI (*Secrétariat Permanent pour la Prévention des Pollutions Industrielles*). Only a few of the forums identified took place at national level. Most were local or regional. All worked as face to face meetings. Since membership of those spaces is generally not public knowledge, interviewees were not approached as members of a specific safe space. Rather, people involved in industrial safety in those sectors were approached, and some of them turned out to be participating in one safe space or another. The picture emerging from the data is therefore, by necessity, partial.

Background

The study presented here looks at two industrial sectors: onshore chemical and petrochemical industries. In both, losses of control over hazardous processes or substances could have catastrophic consequences. In fact, major accidents have occurred in both sectors, even at well resourced firms, and in spite of very advanced technical, managerial and regulatory tools being applied.[1]

Due to various characteristics of these industries, they may experience losses of control over hazardous processes – which I will refer to as 'incidents' – on a rather frequent basis (sometimes several times per week for a large site, such as a refinery). Within the community of process safety specialists, many have argued for decades that such 'small' events constituted important sources of information, to learn and prevent larger scale, catastrophic events. Regulators have generally adopted that view as well. As a result, when national regulatory authorities in EU countries have been inspecting businesses presenting such characteristics, they have increasingly requested evidence that incidents were being recorded and analysed, and lessons were learnt and implemented.

Information on incidents can be used to build databases, which can then be relied on for intelligence (e.g. Lisbona et al. 2012), or scenario analysis, to input frequencies on types of events when assessing the probability of accident scenarios. Another possible use of incident information is benchmarking, to help industry and regulators assess one firm's safety performance against another's. Incidents can also be used for enforcement. Although incidents may be unforeseeable occurrences for which no one can be blamed (that is due to the 'unruly' character of technologies used in those sectors; Wynne 1988), they may also result from negligence and intentional breaches of standards or regulations. In that respect, incident reports may also contain 'guilty knowledge'. As a result, regulators and businesses would generally view incidents as a regulatory and reputational risk.

These concerns should be seen against a backdrop of institutions and processes encouraging transparency from regulators and business organizations. Many countries have passed Freedom of Information (FOI) legislation (in 2000 in the UK), which has made most information in the hands of public authorities communicable on request to

[1] The BP Texas City accident is one of the recent catastrophes that could have been prevented, had knowledge of past failures been effectively shared and incorporated into the refining operations of BP in the United States (Hopkins 2008).

members of the public.[2] Transparency principles have also been extended to industry, notably in the domain of technological risks, in the form of so-called ‘right to know’ policies: those have emerged in the United States and Europe to improve the sharing of relevant risk information between companies and workers, subsidiaries, sub-contractors, regulators, public interest groups, other companies, or neighbours (Baram 1984; Gouldson 2004; Jasanoff 1988; Walker et al. 1999). In France, for instance, there has been a consistent push from Non-Governmental Organizations (NGOs) for more and better information of the public in relation to a wide variety of risks (Suraud 2014). In other words, the already sensitive character of incident information for industry and the regulator is further heightened by external demands for transparency.

Data

This study found safe spaces to be designed and to operate in a way that would make participants ‘safe’ from three main risks: a reputational risk that may result from exposure to the public, peers, or regulators; a reputational and legal risk that may result from regulatory enforcement, including the possibility of criminal prosecution; and a competition risk that may result from either antitrust authorities targeting the industry on suspicion it has been organizing a cartel, or from firms trying to gain competitive advantage over their peers. The data collection phase was certainly informed by the existing literature on incident reporting, therefore the idea that issues of transparency and accountability might matter for businesses sharing incident data – discussed by Reason (1997), Innes (2001) or Stafford (2007), among others – had been included in interview guides. However, the matter of competition was not considered initially; it emerged from the interviews.

Transparency

When incident information may be shared by businesses with third parties, the issue of its publicness is central. Key to many interviewees’ concerns is the reputational impact that incident information might have for the company and the sector sharing it. Thus, a French inspector summarized how many industry managers viewed plans to make more incident data available to the general public: ‘we do not want our plants to be perceived as bedlams’.

Yet, selective transparency about failures towards peers (rather than the general public) has also been hailed within the profession of safety specialists as a means of sharing lessons learned and averting disastrous accidents. Indeed, many interviewees mentioned that, as trained safety engineers, ‘they would want to share everything’ with their peers. Accordingly, reluctance to share would sometimes be attributed to non-safety professionals, and notably ‘lawyers’, who would tend to have greater clout within US-based companies. Lawyers, according to several interviewees, would be particularly concerned with the risks that sharing too much information might imply for the brand’s reputation. Such concerns are heightened further when information initially shared at closed meetings is considered for publication to a wider audience.

[2] As of 2015 there have been consistent signals that the UK government considered weakening FOI legislation (Stacey and Pickard 2015).

> At the engineering level, everybody wants to share everything. But when it comes to publishing on our website to the world, the lawyers get nervous. … Lawyers are concerned about reputation to the industry, what the regulator is going to say, what expectations they are going to have.
>
> (Trade association, oil, UK)

To accommodate these concerns, the sharing of incident information between organizations may be made 'safe' from transparency demands through two principal means. The first consists in restricting access to the discussions and the second in removing identifiers from the information shared during those discussions.

In the UK, all meetings where interviewees discussed incidents were closed meetings. They would not be advertised publicly. In fact, since they would generally be either organized or moderated by a trade association, only members of the trade association would attend. In a minority of cases only, a representative of the British regulatory agency would also attend meetings when incident information would be shared (see next section). However, that would not imply that the contents of the meetings could be shared widely afterwards, via the regulatory agency or any other route. Trade associations or meeting chairs would generally ensure that any information they might then share with others should not include identifiers.

> It depends on the group you are with, and how cautious certain trade associations are in the way they share things. There is an understanding that this should not be traceable to any particular organization.
>
> (Safety manager, UK)

British industry demands for anonymity have led to disputes on publishing aggregate figures on process safety performance with identifiers.[3] As an example of how this reluctance and regulatory demands for incident data sharing was reconciled, the British trade association for downstream oil and gas industries opted for two levels of reporting on safety incidents its members were willing to share: an internal one with substantial detail, in the form of Process Safety Information Notes, and a much more generic reporting to the outside world, in the form of Process Safety Alerts.[4]

The varying sensitivities and compromises around secrecy appear more clearly when comparing regulatory efforts to gather incident data in France and the UK, even and especially when they did not involve setting up 'safe spaces'. In the mid 2000s, the British HSE strived to directly collect detailed qualitative information on a type of incidents (losses of containment) in the chemical and petrochemical industries. Although that did not involve setting up meetings but called businesses to voluntarily

[3] Such reluctance is not specific to the British industry. The experience of the American Chemistry Council on publicly reporting nominative figures for process safety events shows a similar reluctance from most firms operating in the US against making such data public; <http://reporting.responsiblecare-us.com/Reports/Members/Sfty_Cmpny_Rpt.aspx>

[4] See UKPIA's website <http://www.ukpia.com/process-safety/process-safety-alerts.aspx>

send the information to the HSE, none of the information could be passed *with identifiers* either to inspectors or to the public[5] so as to circumvent FOI legislation.[6] These strict conditions were apparently criticized from within the HSE, as the information could contain 'guilty knowledge' (interview with two regulators, UK). The project was eventually discontinued, and the task of collecting such data passed to a trade association.

In France regulators requested from industry more transparency than their British counterparts when, in the early 1990s, they set up ARIA, a public database of incidents. ARIA has been fed principally with information received by local inspectors from businesses, as per the latter's legal obligation to self-report such events, rather than via a 'safe space'.

> The principle is that we never publicly show the name of the company or of the factory. But we show the location. The goal is: no name. That was a condition for industry owners to accept this database.
>
> (Regulator, France)

Fully accessible to the public,[7] the description of each event has included date, location, and some details of the process and/or the substances involved. In that respect, anonymity has been mostly symbolic: the information provided would be generally sufficient for a motivated reader to identify which firm experienced which incident. Business concerns about the way information might be used have been alleviated otherwise, by giving the firm the ability to validate incident descriptions before they were put online.

> … incident descriptions are verified: we send them to the local inspector, and in parallel to the trade association, which then does its own verification with the owner. We take proposed modifications into account only if they are justified.
>
> (Regulator, France)

[5] There have been precedents where NGOs obtained and published data which firms had provided to regulators (Gouldson 2004: 142).

[6] Braithwaite (1982: 1487) reports that the US Food and Drugs Administration in the 1970s immunized pharmaceutical industry reports from compliance with Good Laboratory Practices from inspectors and Freedom of Information Act (FOIA) requests. The INPO and the FAA's VDRP have similarly ensured secrecy against right to know principles and FOIA (Rees 1994; Mills and Reiss 2014).

[7] See ARIA website <http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en>

Table 1. Manufacturing industry incidents recorded in the ARIA database for the PACA and NPDC regions between 1996 and 2013.

	1996-1997	1998-1999	2000-2001	2002-2003	2004-2005	2006-2007	2008-2009	2010-2011	2012-2013
PACA	41	48	20	107	114	120	195	112	91
NPDC	54	43	50	61	100	62	70	65	60

Source: ARIA database.

Comparing the ARIA database, which is not the output of a 'safe space', and the information the HSE collected by offering full secrecy to firms, both contained similar (and equally variable) levels of information detail.[8] Perhaps instructive in that regard is the regular publication in the French region of Provence-Alpes-Côte d'Azur (PACA) of incident information that includes identifiers and has been freely accessible on the internet.[9] When contrasting the number of incidents published in ARIA that took place in PACA and those in another region with a reasonably similar population of hazardous sites (Nord Pas-de-Calais, NPDC),[10] but with a lesser degree of transparency, one finds that PACA has had a distinctly better incident sharing outcome from the early 2000s onwards (Table 1). This suggests that greater transparency has not been a fundamental obstacle, while the consistent pressure applied by the local branch of the Inspectorate (IIC) on the local industry to share more information appears to have paid off (interview with trade association representative; interview with regulator, France).

Other factors could account for this variation such as economic factors affecting firms based in one region and not another, but these were not specifically examined in this study. Nonetheless, the trend suggests that secrecy might not be a sufficient or necessary condition for information flow between businesses and regulators. The impact of secrecy on the quantity and quality of the information exchanged between businesses was also unclear. Interviewees were generally quite nuanced in their assessment of exchanges between businesses taking place in closed meetings. Some testified to the occasionally exceptional levels of sharing (and mutual challenge) they witnessed. Others expressed scepticism, suggesting that levels of information sharing varied significantly despite the secrecy granted by the safe space, which implies that individual participants or other factors were to blame.

In sum, making information sharing 'safe' from transparency may effectively translate into various compromises, from full secrecy to symbolic forms of anonymity. These compromises suggest that the actual level of secrecy obtained and observable

[8] Whether and how either was useful to regulators or industry was not plainly obvious.

[9] See the website of CYPRES, a tripartite body (regulator, industry and NGOs) addressing risks in the region; <http://www.cypres.org/documentation/publications-du-cypres/risquinfos-cypres/>

[10] As of 2012, PACA had 48 'high tier' sites, NPDC had 46 and both had had 24 'low tier' sites. PACA had 1,199 other sites that were neither high nor low tier, yet required a license to operate. NPDC had 1,430 such sites. Source: French Ministry of Ecology, Sustainable Development and Energy, <http://www.installationsclassees.developpement-durable.gouv.fr/rechercheICForm.php>

empirically is a social construction that combines multiple influences. In other words, stakeholder views on the level of secrecy actually needed might be a far cry from the actual risks of an adverse public response,[11] and their relationship to actual levels of data sharing may be weak. Compromises around secrecy might provide indications of the power of industry relative to regulators (and other pro-transparency audiences). It may also reflect different views on the legitimacy of private or public-private types of governance.

Accountability / Enforcement

Enforcing agents and courts would generally be mandated to ensure that organizations breaching public rules are held accountable, and courts would often be able to sanction enforcement authorities (either as administrative courts where they exist or through judicial review) if they did not perform their legal duties. Information sharers may similarly be threatened, since the information they share may contain evidence of breaches of legislation. In France and the UK, there are no explicit guarantees of immunity offered to industry as a means to create 'safe spaces'. The official stance of regulatory authorities has been that any shared piece of information might lead to an enforcement response; such statements can be deemed to reflect widely shared norms that firms should always be held accountable for breaches. Accordingly, business interviewees in both countries voiced concerns that sharing could lead to sanctioning. For example:

> If the consequence of that is to get sanctioned like a child who has done something wrong, then it fails to produce transparency (former representative of trade association, France).
>
> Unless it reveals something awful, it's important that [regulators] do not prosecute … they have got to make it worthwhile [for businesses to be transparent].
>
> (Safety manager, UK)

These concerns have been alleviated by mostly informal means.

In the UK, the 'Chatham House Rule', as it is known after an international relations think tank, has been one of the means to reassure participants of some 'Responsible Care cells' (moderated by the Chemical Industries Association) that they would not be held accountable for the information they shared. The rule states:

> When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.
>
> (Chatham House, Royal Institute of International Affairs)

[11] Previous work on information disclosures have recorded a mostly apathetic response from the public (Kraft et al. 2011; van Erp 2011).

Such a rule would notably prevent any enforcement response. Participants would be reminded of the rule at the start of meetings.

> The rules are: whatever is discussed, the [regulators] could not use it. It's a gentleman's agreement.
>
> (Safety manager, UK).

With the informal guarantee embodied by the rule, some RC cells have admitted a representative from the regulatory agency to the part of the meeting when incidents would be discussed. In other cells, however, regulators would be admitted only to the rest of the meeting, when no incident information would be shared. The extent to which the Chatham House Rule might enable extensive sharing of information in spite of the regulator's presence at the meeting is difficult to gauge, although a few interviewees considered that it worked. One HSE inspector who had been attending such meetings observed that sharing would sometimes be extensive, as participants 'would put their wounds open for others to see'. Much would depend on the regulator's agreement not to follow up meetings with inspections or investigations, even if the information heard appeared to justify it. As the quotes below suggest, that would be a matter of the industry's expectations and of the regulator's readiness to accommodate them, and vice versa.

> Obviously, if something horrendous – we'd have to say, look, we got to stop, now. What you've just told us has gone beyond what we can accommodate in an off-the-record kind of discussion.
>
> (Regulator, UK)

> I have experienced meetings where the inspector there was taking notes, saying 'I will go visit them'. … Certain enforcement agencies are using this for information gathering.
>
> (Safety manager, UK)
>
> .
>
> [The members of the RC cell] have determined that [the presence of a representative from the regulator] inhibits some discussion. … Sometimes they might want to talk about what [regulators] call 'guilty knowledge': problems not reportable but which are attracting attention.
>
> (Trade association, UK)

The restraint expected from regulators would not be specific to 'safe spaces', however. It might also be expected from them in the field, and their behaviour in one context might indeed condition their access to another. Thus, an inspector breaching these expectations in the field might also be considered unfit for RC cell meetings. A safety manager recalls a debate within an RC cell on deciding not to admit an HSE representative to discussions around incidents:

> The local regulators went around, looking through your accident record. … People were very upset, they perceived they were unfairly pilloried. … The inspectors threatened regulatory action, people felt affronted.
>
> (Safety manager, UK)

Indeed, an inspector may not hold a business accountable for its failures and breaches if it shared extensive information about them. For instance:

> Our personal experience is that if you've done a full investigation and share it with them that's usually it. … They normally only take it further and prosecute when they believe it's in the public interest to prosecute. And that isn't – normally, that's only going to happen if there's gross negligence or you'd not done the investigation properly and you've missed half of the story.
>
> (Safety manager, chemicals, UK)

However, dispositions towards sharing might wane when inspectors would not show 'understanding'.

> They liked it to be open and they like to see the full report, and they treated it like, 'Well, we can see that you're open and honest with us, and therefore, it's okay. We're not going to go taking advantage of it.' But the attitude in the last – certainly since I've been here, and probably the year before, had changed, so the last four years has changed to 'now we can actually get you for something, and you give us the information so we can do it, and we're going to get you. We're going to prosecute you.'
>
> (Safety officer, UK)

Likewise, one industry operator's openness in RC cells might convince the regulator in attendance that this should not be followed up with enforcement action. It might take a certain kind of regulator to accommodate the concerns of businesses, notably by showing understanding rather than responding to information sharing with investigations or enforcement.[12]

In sum, the risks of being investigated or sanctioned for sharing information may be dealt with in different ways. Immunity rules might be formally drawn (as in a few cases documented in the US), or it might be granted informally subject to unclear limits that would be a matter of regulatory discretion, and may be negotiated between the industry and enforcement authorities. Hence, the workings of safe spaces on this aspect would

[12] Earlier socio-legal studies have shown that a good deal of self-reporting occur under informal rather than formal guarantees of immunity, anonymity or leniency, and alongside formal provisions that violations should be sanctioned. The discretion left to enforcing agents and the scope for informality that exists in many regulatory encounters may sometimes allow for sensitive information to be exchanged between the business and the enforcement agent, without it being recorded or acted upon (e.g. Haines 1997; Hawkins 1984).

be closely linked with other features of their environment, and particularly the 'routine' processes of controlling for breaches of regulations and sanctioning.

Competition

The third risk in 'safe spaces' might be designed to protect their members from is the risk of unfair competitive practices: either anti-competitive behaviour or excessive competition.

Antitrust legislation, according to Djelic (2005), constitutes a 'global structuring frame' for economic activities, embodied in Europe in European Union competition law, as included in the Treaty of Rome (1957). Gatherings of representatives of firms that operate on the same market may be viewed with suspicion by antitrust authorities the said representatives could use 'safe spaces' as an opportunity to collude to the consumers' disadvantage. There are legitimate concerns in this area because of enforcements against numerous cartels in the chemicals industry in the past decade in Europe (BBC 2006; European Commission 2009; Info Chimie 2013).

> There's a fear of sharing information that puts you at risk of being accused of organizing a cartel.
>
> (Safety manager, oil, UK)

Some sub-sectors could be particularly vulnerable to the risk of collusion because of a limited number of players producing similar products and targeting similar clients. The paradox is that the potential for joint learning within safe spaces would be the greatest within such coherent sub-sectors. For example, numerous interviewees in France mentioned the case of Eurochlor, the association of chlorine producers, as a model of inter-organizational learning around incidents. According to them, coordinated sharing of information enabled significant progress in making that particular sub-sector safer.

Fragmentation, however, would make information exchange and cross-learning exercises difficult, or even impossible. Thus, Eurochlor's achievements were commented on as an outdated model, because of the increased pressure of financial investors on company structures and strategies.

> It worked in the 1980s, for instance with Eurochlor. Then in the 1990s financiers bought back everything and it sank.
>
> (Regulator, France)

> The chlorine people have gone their separate ways. … With the fragmentation of the industry it becomes more and more difficult to exchange well.
>
> (Safety manager, France)

Accordingly, interviewees sometimes lamented that RC cell meetings may gather together businesses with such diverse profiles that there could not be meaningful sharing of information with each another.

In the UK, the risk of anti-competitive collusion has been addressed by trade association representatives, who have taken it upon themselves to remind participants that they should abide by European antitrust rules.[13] For example, the minutes of a RC cell meeting begin with the following statement:

> [The representative of the Chemical Industries Association] outlined the requirements for an updated CIA approach to anti-competition compliance. Whilst the subject matter of CIA's Responsible Care cell meetings focuses overwhelmingly on issues free from competition concerns, for good order all present are reminded of the need to comply with EU anti-competition (sic) laws. The meeting, and any side discussions, should not cover discussion of product market details, pricing, cost structures, etc. If discussions were to tend towards these matters then the meeting would be stopped. All are empowered and encouraged to intervene in such an event.

Such provisions would address only some of the implications of safe spaces for the objective of maintaining fair competition within a given sector. Safety managers were also conscious that competitors might use incident information to their advantage. Such concerns are present in sectors where incident narratives might include proprietary information (for instance, 'recipes' in the pharmaceutical sector). But they are also present where there is both low innovation and homogeneity (as in the fertilizers industry or refining).

> There is resistance. It's particularly difficult in our sector because all our members are in direct competition with each other.
>
> (Trade association, downstream oil and gas, UK)

In such circumstances, information that outsiders would consider benign (such as the throughput at an oil and gas terminal for example) might be sensitive nonetheless. Trade association representatives would act to protect information sharers, with the threat that those who would not comply could then be reported to public authorities, and/or see their membership rescinded.

> You can have a situation where somebody could be talking about … some problem that their site has had. And if you can turn that around and use that to a competitive advantage, it … at the end of the day, all the companies are in the business to make money. So, you know, that's why we control it very well, and very keenly. … They've got the knowledge that they can actually share that information that, 'Oh, well,

[13] Similar issues arose in relation to voluntary initiatives whereby food industry companies gathered to discuss best practices to improve the environmental sustainability of the sector (Food Ethics Council 2011).

> we have made a mistake. Our systems were not as robust as we thought they were, but we're now fixing it.'
>
> (Trade association, chemicals, UK)

In other words, each participant and the trade association hosting the meeting would be entrusted with the information under the explicit caveat that they accepted and effectively agreed to protect the business' position of competitors.

> I have heard: 'Please don't take that out because of competition issues.'
>
> (Regulator, UK)

The tension between competition and information sharing becomes even more of a challenge when participants come to see the understanding of an incident and the solution they found to prevent it from occurring again as a competitive advantage in itself. There would be reluctance to share, as firms might consider that the benefits of the work they have put into solving a problem should not be given freely to competitors.

> We will discuss lessons learned but not the specifics. I wouldn't share how this was resolved. It's not down to me to tell a company how to mitigate an issue. … Just as we are ruthless in safety we have to be ruthless in business.
>
> (Safety manager, chemicals, UK)

Breaching standards and regulations (which could contribute to incidents) might also sometimes give a firm an advantage over other compliant businesses. In that regard, such forums might also enable a level of mutual checking, and thus contribute to enforcing a satisfactory level of competition. For example, the industry-only forum for the fertilizer industry (known as 'AN-NA') was 'designed to give a level playing field' for everyone within that sector according to a consultant in the UK for the fertilizer industry. Similarly, in one of the chemical industry forums:

> If you've got somebody who is doing something totally different that is actually illegal or very dangerous, they may get a competitive advantage over everybody else; so they're all trying to work towards the same standards, and making sure that one is not applying this standard to the detriment of their business because somebody else is doing it.
>
> (Trade association representative, UK)

In sum, competition would shape the way sensitive information could be shared among businesses in multiple and sometimes contradictory ways. On the one hand, one's experience of an incident might be construed as a competitive disadvantage if it revealed a temporary weakness to one's competitors. On the other hand, an incident might also be construed as a competitive advantage if others were left to find a solution to the problem revealed by the incident, without any cues from the sharer. Similarly, a forum where such information could be exchanged may be a means to construct a level playing field between competitors, but it could also be used to organize anti-competitive practices. These mixed views and expectations are likely to lead to a good deal of strategic disclosures and non-disclosures within safe spaces, and certainly to significant variations in the quality of participant contributions.

Discussion

This paper has provided a glimpse of the extensive variety of arrangements characterising safe spaces. The study has identified an array of socially constructed compromises between industry, regulators, and an environment of constraining expectations, reflecting tensions between what participants to safe spaces may share with one another, and what their environments would expect them to do: be transparent, be accountable, and trade fairly.

These compromises appear to be reflecting macro-level variables, such as the relative tolerance for business-state collaboration to resolve matters of public interest. Public attitudes – themselves shaped by existing institutions – may vary a great deal on this matter, for instance between the northern and southern parts of Europe (the former being usually more accepting of public-private governance than the latter). Similarly, attitudes towards immunity or secrecy deals for industry might vary significantly between countries, opening up or closing down possibilities for setting up safe spaces. Antitrust controls also vary in strength, and the credibility of antitrust enforcement authorities may also differ, shaping the extent to which antitrust concerns could contribute to the shape and workings of safe spaces.

Another set of factors to consider is the power imbalances between industry and regulators, compounded by the support each may obtain from other important stakeholders such as elected national representatives. For example, the evidence reviewed earlier suggests that countries with a more liberal orientation and a weaker state, like the UK, might be less willing and have less power to shape safe spaces in ways that would constrain industry, than countries with a more statist orientation and a stronger state altogether, like France. The industry's own capacity to organize, but also the way industry organizations such as trade bodies operate (either as a lobby where influence moves from the bottom up, or as a structuring, leading force, where it moves from the top down), would also likely determine what safe spaces would look like or what they could achieve.

Perhaps tautologically, tensions between participants at safe spaces and their environment are at the heart of safe spaces; external demands addressed to business organizations are the reasons why safe spaces exist. In the absence of any safe space, as organization theorists might argue, organizations would address these demands with secrecy, releasing information only strategically. Pfeffer and Salancik (1978: 105) have argued that 'many organizations find secrecy a necessary condition for maintaining the discretion required to operate within a set of conflicting demands. The latitude afforded for complying or not complying is important'. Besides, 'organizations will release information when it is in their best interests to do so and will attempt to obtain information that enables them to exercise influence. What information is available about organizational actions is the outcome of a political process' (ibid: 106; also Brunsson 2002).

Safe spaces are meant to circumvent such default business attitudes towards secrecy and strategic communication. But do they? The evidence presented in the empirical section is mixed. While some interviewees reported cases of extensive sharing, several others showed or reported persistent reluctance to share extensive information with others, even within the boundaries of safe spaces. To some extent, this reflects the counteracting influence of the broader environment. Thus, while regulators would often be expected to abide by and enforce principles of transparency, accountability and competition, acknowledging or supporting safe spaces would often involve that they actually 'buffer' regulated businesses (Pfeffer and Salancik 1978: 106) from one at least of those principles, the organizations that defend them (e.g. the judiciary, the media), and the general public. For a regulator to play that role may be opposed by members of the regulatory agency, and by the latter's important external audiences (e.g. the media, political principals, NGOs). To maintain safe spaces and its reputation in the eyes of important audiences at the same time, a regulator would have to project ambiguity, both internally – towards its own enforcement staff – and externally (Carpenter and Krause 2012). As a result, immunity for sharers may not be unconditional. It would not be experienced as such by firms being investigated or sanctioned outside safe spaces and they might then refuse to share information with regulators within safe spaces.

Formally established secrecy towards third parties (i.e. other than industry or regulators) – a key feature of safe spaces – does not appear to be a fully effective aspect either. Even participants to closed meetings spoke of poor sharing practices and blamed other issues than safe space design (e.g. industry fragmentation) for it. However, there are indications that some information sharing processes offering little secrecy to the sharer have been yielding good levels of information. That would include regulatory encounters outside any safe space, where information is sometimes exchanged without much more than an informal, shared understanding that it will not be recorded or acted upon. In other words, formally shielding businesses from the wider world might be less of a necessity than the idea of safe spaces implies.

The mixed evidence recounted earlier also shows how participants in safe spaces, even though they are encouraged not to share and use information, remain acutely aware of the value of that information, which they sometimes share and use strategically. Thus, one reason for participation is to check on one's competitors. In other words, other participants of safe spaces might still be a cause for concern rather than trust, inspiring strategic communication rather than openness. This shows that, while safe spaces aim to cut off environmental demands, thus removing some of the obstacles to information sharing, incompatible demands and goals would still be brought to the safe space by participants themselves. As a result, participants may share only sparingly, or act on the information heard in ways that would discourage future sharing.[14]

[14] Arguably, preventing any face to face interaction between participants and relying instead on a third party to sanitise information received before sharing it (e.g. Elliott 2014) might be a way around this

Arguably, regulation scholars and public administration scholars have already discussed solutions to this problem. They have advocated the necessity for regulatory agencies to create effective internal barriers between those engaged with industry for intelligence gathering and information sharing, and those in charge of investigations and enforcement (e.g. Braithwaite 1998). One could imagine similar dispositions within industry with its representatives participating in safe spaces having the mandate to exchange extensively on matters of common interest, free from the veto of other internal constituencies (e.g. legal teams) and with the obligation not to use the information against those who shared it. For that to happen, however, firms would need leaders committed to sharing information so as to achieve collective interests. In other words: socially responsible CEOs and boards, sharing a common ‘industrial morality’[15] (Gunningham and Rees 1997). Is there any evidence of such a shared ‘industrial morality’? Very little (Lytton 2014; Rees 1994). As far as the sectors considered in this study are concerned, the argument by Hoffman (1999) that there has been a change of heart in the chemical industry, leading to an embrace of pro-environmental norms, has not been vindicated. Rather, there has been much scepticism about the RC initiative since its launch in the 1980s. Is the emergence of an industrial morality a matter of time? That is unlikely. Arguably, it might be difficult for industrial morality to emerge, spread and become embedded into industrial networks, when those networks are global, structured around principles of financial profitability rather than around common core functions and issues, and when they are subject to frequent restructures due to market fluctuations.

These observations suggest that inter-organizational safe spaces may be rarely effective for long, if at all, either for gathering intelligence or for industry self-regulation; they are inherently constrained, not only from the outside, but also from within. Therefore, one would not expect them to become institutionalized. In other words, the more likely outcome for safe spaces is for them to remain imperfect attempts to connect different practices and views together, without ever reconciling them. This could explain the ongoing exceptionality of the INPO, an institutionalized and successful safe space that has not yet found its match.

The above provides the first elements for a theory of safe spaces. In a nutshell, safe spaces are primarily shaped against the demands that key audiences address to industry and regulatory agencies. However, these demands are also filtered by the participants’ own perception of those demands and how they might conflict with their self-interest. Differences between participants, particularly their mixed and sometimes incompatible goals are another significant element, as they may encourage strategic behaviour within safe spaces. Such differences may notably result from the structures of ownership and levels of integration within a given sector. Thus, whether the industry is concentrated or

issue. This would not prevent inter-subjective conversations taking place, assuming another safe space for those was also provided.

[15] For Gunningham and Rees (1997: 380), industrial morality involves businesses adhering to norms that ‘challenge traditional ways of doing business [i.e. profit maximization only] and redefine the industry’s responsibilities in light of social values widely shared *outside* the industry’.

fragmented, and whether it is vertically or horizontally integrated, are likely to make safe spaces more or less difficult to set up and organize. It will also conceivably determine the industry's appetite for safe spaces. Numerous features of safe spaces, and particularly the way they are led (including various formal and informal strategies to deflect obstacles to information sharing), may reinforce or rather weaken the contribution of the above mentioned factors to information sharing. Overall, the above implies that there is no sufficient relationship between the 'safe' character of safe spaces and the level of information that is shared between them. There might not even be a necessary relationship between, for instance, secrecy and information sharing. Arguably, secrecy might contribute to information sharing if certain conditions were present, or there might equally be information sharing without much secrecy, depending on the conditions. Future research should strive to ascertain what these conditions are, and more generally expand our still limited understanding of safe spaces.

Conclusion

This paper has presented a study on inter-organizational safe spaces, where business organizations and, sometimes, regulators too, would meet and exchange information, safe from the constraints and expectations of various third parties. This kind of safe spaces have been very rarely studied and is therefore, poorly understood. One study (Rees 1994) may have given the impression that safe spaces could operate as self-regulatory institutions, effective at achieving a high quality of exchanges and behavioural changes to resolve public interest issues within a given industry sector. This paper has provided a much more mixed evidence, that rather points to the fragility and contingency of these safe spaces, and to the existence of multiple, and often probably irremediable obstacles to their institutionalization. These findings and interpretations suggest that the promises of inter-organizational 'safe spaces' should not be overestimated. Most inter-organizational safe spaces might be unsustainable and/or perform poorly, unless they are constantly stimulated by committed individuals, itself a highly contingent variable. Safe spaces conducted by industry bodies, such as RC cells, have thus fluctuated much over the years, for instance in the UK, in parallel with the commitment of industry and regulators to tackle industrial hazards. Safe spaces should not be readily considered useless or unwarranted, even if they could be one or the other. However, they are a limited way of addressing the information challenges presented by the need to regulate numerous, complex issues developing in a globalized economy.

References

Baram, M.S. (1984) 'The right to know and the duty to disclose hazard information', *American Journal of Public Health* 74 (4): 385–90.

Barnett, M.K. and King, A.A. (2008) 'Good fences make good neighbors: a longitudinal analysis of an industry self-regulatory institution', *Academy of Management Journal* 51(6): 1150–70.

Beaumont, P.B. (1979) 'The limits of inspection: a study of the workings of the government wages inspectorate', *Public Administration* 57: 203–17.

Braithwaite, J. (1982) ‘Enforced self- regulation: a new strategy for corporate crime control’, *Michigan Law Review* 80: 1466–1507.

Braithwaite, J. (1998) ‘Institutionalizing distrust, enculturating trust’, in V. Braithwaite and M. Levi (eds), *Trust and governance*. New York: Russell State, pp. 343–75.

Brunsson, N. (2002) *The organization of hypocrisy*. Copenhagen: Copenhagen Business School Press.

Carpenter, D. and Krause, G.A. (2012) ‘Reputation and public administration’, *Public Administration Review* 72: 26–32.

Chikudate, N. (2009) ’If human errors are assumed as crimes in a safety culture: a lifeworld analysis of a rail crash’, *Human Relations* 62 (9): 1267–87.

Dekker, S. and Laursen, T. (2007) ‘From punitive action to confidential reporting: a longitudinal study of organizational learning from incidents’, *Patient Safety & Quality Healthcare* 5: 50–56.

Djelic, M.L. (2005) From local legislation to global structuring frame: the story of antitrust’, *Global Social Policy* 5(1): 55–76.

Elliott, C. (2014) Elliott Review into the integrity and assurance of food supply networks – final report. London: HM Government.

EPA [Environment Protection Agency] (2000) ‘Incentives for self-policing: discovery, disclosure, correction and prevention of violations’, *Federal Register* 65: 19618–627.

Erp, J. van (2011) ‘Naming and shaming in regulatory enforcement’, in C. Parker and V.L. Nielsen (eds), *Explaining compliance: business responses to regulation,* Cheltenham: Edward Elgar, pp. 322–43.

Etienne, J. (2015) The politics of detection in business regulation’, *Journal of Public Administration Research and Theory* 25: 257–84.

Faure, A.M. (1994) ‘Some methodological problems in comparative politics’, *Journal of Theoretical Politics* 6 (3): 307–22.

Feldman, Y. and Lobel, O. (2011) ‘Individuals as enforcers: the design of employee reporting systems’, in C. Parker and V.L. Nielsen (eds), *Explaining compliance: business responses to regulation,* Cheltenham: Edward Elgar.

Food Ethics Council (2011) ‘Competition and collaboration: the law, food businesses and the public interest’, Report of the Business Forum meeting on 22 March 2011. <http://www.foodethicscouncil.org/uploads/publications/businessforum110322.pdf> Accessed 21 May 2015.

Gerring, J. (2004) ‘What is a case study and what is it good for?’, *American Political Science Review* 98 (2): 341–54.

Gouldson, A. (2004) ‘Risk, regulation and the right to know: exploring the impacts of access to information on the governance of environmental risk’, *Sustainable Development* 12: 136–49.

Gunningham, N. and Rees, J. (1997) ‘Industry self-regulation: an institutional perspective’, *Law & Policy* 19 (4): 376–80.

Haines, F. (1997) *Corporate regulation: beyond ‘punish or persuade’*, Oxford: Clarendon.

Hawkins, K. (1984) *Environment and enforcement: regulation and the social definition of pollution*. Oxford: Clarendon.

Helland, E. (1998) ‘The enforcement of pollution control laws: inspections, violations, and self-reporting’, *Review of Economics and Statistics* 80 (1): 141–53.

Hoffman, A.J. (1999) ‘Institutional evolution and change: environmentalism and the U.S. chemical industry’, *Academy of Management Journal* 42 (4):351–71.

Hopkins A. (2008) *Failure to learn: the BP Texas City refinery disaster*. Sydney: CCH Australia.

Innes, R. (2001) ‘Violator avoidance activities and self-reporting in optimal law enforcement’, *Journal of Law, Economics, & Organization* 17: 239–56.

Jasanoff, S. (1988) ‘The Bhopal disaster and the right to know’, *Social Science & Medicine* 27 (10): 1113–23.

Johnson, A.N. (1996) ‘Blame, punishment and risk management’, in C. Hood and D.K.C. Jones (eds), *Accident and design*. London: Routledge pp. 72–83.

King, A.A. and Lenox, M.J. (2000) Industry self-regulation without sanctions: the chemical industry’s Responsible Care program, *Academy of Management Journal* 43 (4): 698–716.

Kraft, M.E., Stephan, M. and Abel, T.D. (2011) *Coming clean: information disclosure and environmental performance*. Cambridge MA: MIT Press.

Lisbona, D., Johnson, M., Millner, A., McGillivray, A., Maddison, T., and Wardman, M. (2012) ‘Analysis of a loss of containment incident dataset for major hazards intelligence using storybuilder’, *Journal of Loss Prevention in the Process Industries* 25 (2): 344–63.

Lobel, O. (2005) ‘Interlocking regulatory and industrial relations: the governance of workplace safety’, *Administrative Law Review* 57: 1070–1151.

Lytton, T.D. (2014) ‘Competitive third-party regulation: how private certification can overcome constraints that frustrate government regulation’, *Theoretical Inquiries in Law* 15: 539–71.

Macher, J.T., Mayo, J.W. and Nickerson, J.A. (2011) ‘Regulator heterogeneity and endogenous efforts to close the information asymmetry gap’, *Journal of Law and Economics* 54: 25–54.

Mills, R.W. (2013) *Incident reporting systems: lessons from the Federal Aviation Administration’s Air Traffic Organization*, Washington DC: IBM Center for the Business of Government.

Mills, R.W. and Reiss, D.R. (2014) ‘Secondary learning and the unintended benefits of collaborative mechanisms: the Federal Aviation Administration’s voluntary disclosure programs’, *Regulation & Governance* 8 (4): 437–54.

Parker, C. (2002) *The open corporation: effective self-regulation and democracy*. Cambridge: Cambridge University Press.

Pfaff, A. and Sanchirico, C.W. (2004) ‘Big field, small potatoes: an empirical assessment of EPA’s self-audit policy’, *Journal of Policy Analysis and Management* 23: 415–32.

Pfeffer, J. and Salancik G.R. (1978) *The external control of organizations: a resource dependence perspective*. New York: Harper and Row.

Prakash, A. (2000) ‘Responsible Care: an assessment’, *Business & Society* 39 (2): 183–209.

Reason, J. (1997) *Managing the risks of organizational accidents*. Farnham: Ashgate.

Rees, J.V. (1994) *Hostages of each other: the transformation of nuclear safety since Three Mile Island*. Chicago: Chicago University Press.

Rees, J.V. (1997) ‘Development of communitarian regulation in the chemical industry’, *Law & Policy* 19 (4):477–528.

Stacey, K. and Pickard, J. (2015) ‘Gove plans freedom of information crackdown’, Financial Times, 21 June. <http://www.ft.com/cms/s/0/3e10b852-15d2-11e5-a58d-00144feabdc0.html#axzz3oQpMswaj> Accessed 1 October 2015.

Stafford, S.L. (2007) ‘Should you turn yourself in? The consequences of environmental self-policing’, *Journal of Policy Analysis and Management* 26: 305–26.

Suraud, M.G. (2014) ‘L’espace public des risques’, *Revue française des sciences de l’information et de la communication* 4.

Vaughan, D. (1990) ‘Autonomy, interdependence, and social control: NASA and the space shuttle challenger’, *Administrative Science Quarterly* 35: 225–57.

Walker, G., Simmons, P., Irwin, A. and Wynne, B. (1999) ‘Risk communication, public participation and the Seveso II directive’, *Journal of Hazardous Materials* 65: 179–90.

Wynne, B. (1988) ‘Unruly technology: practical rules, impractical discourses, and public understanding’, *Social Studies of Science* 18: 147–67.

Websites

American Chemical Council. ‘Responsible Care: safety report’, <http://reporting.responsiblecare-us.com/Reports/Members/Sfty_Cmpny_Rpt.aspx> Accessed 28 October 2014.

ARIA <http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en> Accessed 19 October 2014.

BBC (2006) ‘EU fines chemicals sector cartel’, 3 May, <http://news.bbc.co.uk/1/hi/business/4968872.stm> Accessed 19 October 2014.

Chatham House <http://www.chathamhouse.org/about/chatham-house-rule> Accessed 19 November 2014.

CYPRES <http://www.cypres.org/documentation/publications-du-cypres/risquinfos-cypres/> Accessed 19 November 2014.

InfoChimie & Chimie Pharma (2013) ‘Des distributeurs épinglés pour un cartel en France’, 3 June, <http://www.industrie.com/chimie/des-distributeurs-epingles-pour-un-cartel-en-france,47025> Accessed 1 October 2015.

European Commission (2009) ‘Antitrust: European Commission fines plastic additives producers €173 million for pirce fixing and market sharing cartels’, Press release IP/09/1695, 11 November. Brussels: European Commision, <http://europa.eu/rapid/press-release_IP-09-1695_en.htm?locale=en> Accessed 1 October 2015.

Ministry of Ecology, Sustainable Development and Energy [France] Base des installations classées, <http://www.installationsclassees.developpement-durable.gouv.fr/rechercheICForm.php> Accessed 6 June 2012.

UKPIA [United Kingdom Petroleum Industry Association] <http://www.ukpia.com/process-safety/process-safety-alerts.aspx> Accessed 28 October 2014.

Centre for Analysis
of Risk and Regulation

The London School of Economics and Political Science
Houghton Street
London WC2A 2AE

tel:	+44 (0)20 7955 6577
fax:	+44 (0)20 7955 7420
email:	risk@lse.ac.uk

lse.ac.uk/CARR