EJIS

RESEARCH ARTICLE

Composting and computing: On digital security compositions

Rocco Bellanova[1]* and Gloria González Fuster[2]

[1]Universiteit van Amsterdam and [2]Vrije Universiteit Brussel
*Corresponding author. Email: r.bellanova@uva.nl

Abstract

Making sense of digital security practice requires grasping how data are put to use to compose the governing of individuals. Data need to be understood in their becoming, and in their becoming *something* across diverse practices. To do this, we suggest embracing two conceptual tropes that jointly articulate the being together of, and in, data compositions: *composting* and *computing*. With composting, we approach data as lively entities, and we explore the decaying and recycling processes inside Big Data security. With computing, we approach data as embodied and embodying elements, and we unpack the surveillance of 'asylum speakers'. Together, composting and computing challenge recurrent images of data. Our conceptual composition takes sound as a necessary sensory counterpoint to popular data visions, notably in light of Ryoji Ikeda's artworks.

Keywords: Composting; Computing; Compositions; Data; Security; Sound

Introduction: Here be digital data

The term 'composition' may seem insufficient to you, but it seems to me that one always makes something with something.[1]

[W]hat we are confronted with are 'bachelor' data: paradoxical givens that are not in reality given to any subject at all, givens that are not really there for anyone, thus contradicting the habitual, phenomenological meaning of the term.[2]

The space is mostly dark; there is no silence.[3] *Bright lights, predominantly white ones, compose geometrical figures. They draw your attention; they are focal sites – they become the object of your cognitive efforts. This is a fully embodied experience. Each artwork is made of sound as*

---

[1]Felix Guattari in Félix Guattari and Oliver Zahm, 'On contemporary art', in Eric Alliez and Andrew Goffey (eds), *The Guattari Effect* (London: Continuum, 2011 [orig. pub. 1992]), p. 45.

[2]Élie During, 'Ikeda, or subliminal time', in Ryoji Ikeda (ed.), *continuum* (Pliezhausen: Éditions Xavier Barral, 2018), p. 59.

[3]This paragraph recounts a visit to the exhibition 'Ryoji Ikeda', at the Eye Filmmuseum in Amsterdam, Netherlands. The visit took place on 19 September 2018. The exhibition displays several works by artist Ryoji Ikeda {www.ryojiikeda.com} accessed 15 October 2018.

much as of visuals. As you walk into the exhibition, sound surrounds you. You find yourself in the middle of an avalanche of blinking digits and moving lines. You nearly feel overwhelmed, and it gets more intense when you approach each installation. The sounds, the lights, they are the by-product of datasets generated for other purposes. As the exhibition brochure puts it, '[Ryoji Ikeda] develops his computer programs and algorithms that generate the images and sounds for his compositions.'[4] Here the datasets work like compost. Most of the datasets were generated by sophisticated devices, but they are collected by Ikeda as if they were 'bachelor data'.[5] They are recycled into abstract visuals and rhythms, seemingly familiar images and noise. There is no (data) composition without some form of computing. This world speaks data and these data are way too embodied.

We live *in medias data*. As Ikeda's compositions show, data inform our world – they can compose our reality, and they arrange us inside it. Security practice is no exception. From smart and biometric border controls to body scanners, from drones to passenger and financial surveillance systems, processing digital data is crucial for (in)security actors.[6] Data and data analytics carry the promise of actionable knowledge, that is, meaningful information for targeted security decisions. Critical security scholars increasingly cater to these 'security devices', investigating their practices and their politics.[7] But, with a few notable exceptions,[8] critical security research fails to question how data come to be part of security compositions. While Critical Data Studies[9] and Surveillance Studies[10] increasingly invite data to be conceptualised as socially *and* materially constructed artefacts, Critical Security Studies (CSS) tends to consider data as the crude foundations of security assemblages, as though data were endowed with obvious representational value. In light of Ikeda's artworks, we summon CSS to explore digital data, to borrow from Lauren Wilcox, as both 'embodied and embodying' elements of security compositions.[11]

---

[4] Eye Filmmuseum, 'Ryoji Ikeda', exhibition brochure (Amsterdam: Eye Filmmuseum, 2018).

[5] During, 'Ikeda, or subliminal time', p. 59.

[6] Louise Amoore, 'Biometric borders: Governing mobilities in the war on terror', *Political Geography*, 25:3 (2006), pp. 336–51; Rocco Bellanova and Gloria González Fuster, 'Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices', *International Political Sociology*, 7:2 (2013), pp. 188–209; Julien Jeandesboz, 'Smartening border security in the European Union', *Security Dialogue*, 47:4 (2016), pp. 292–309; Mark Salter, 'Passports, mobility, and security', *International Studies Perspectives*, 5:1 (2004), pp. 71–91; Lauren Wilcox, 'Embodying algorithmic war', *Security Dialogue*, 48:1 (2017), pp. 11–28; Matthias Leese, 'The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue*, 45:5 (2014), pp. 494–511; Marieke de Goede, 'The politics of preemption and the war on terror in Europe', *European Journal of International Relations*, 14:1 (2008), pp. 161–85.

[7] Anthony Amicelle, Claudia Aradau, and Julien Jeandesboz, 'Questioning security devices: Performativity, resistance, politics', *Security Dialogue*, 46:4 (2015), pp. 293–306.

[8] Louise Amoore, 'Data derivatives: On the emergence of a security risk calculus for our times', *Theory, Culture & Society*, 28:6 (2011), pp. 24–43; Claudia Aradau and Tobias Blanke, 'The (big) data-security assemblage: Knowledge and critique', *Big Data & Society*, 2:2 (2015), pp. 1–12; Mareile Kaufmann, Simon Egbert, and Matthias Leese, 'Predictive policing and the politics of patterns', *The British Journal of Criminology*, 59:3 (2018), pp. 674–92.

[9] Craig Dalton and Jim Thatcher, 'What does a critical data studies look like, and why do we care? Seven points for a critical approach to "big data"', *Society and Space* (2014), available at: {https://societyandspace.org/2014/05/12/what-does-a-critical-data-studies-look-like-and-why-do-we-care-craig-dalton-and-jim-thatcher/} accessed 16 April 2019; Andrew Iliadis and Federica Russo, 'Critical data studies: an introduction', *Big Data & Society*, 3:2 (2016), pp. 1–7; Rob Kitchin and Tracey Lauriault, 'Towards Critical Data Studies', in Jim Thatcher et al. (eds), *Thinking Big Data in Geography* (London: University of Nebraska Press, 2018), pp. 3–20.

[10] Tobias Matzner, 'Beyond data as representation: the performativity of big data in surveillance', *Surveillance & Society*, 14:2 (2016), pp. 197–210; José van Dijck, 'Datafication, dataism and dataveillance', *Surveillance & Society*, 12:2 (2014), pp. 197–208.

[11] Wilcox, 'Embodying algorithmic war', p. 13.

This contribution is a conceptual composition. We speak to CSS by bringing together research and notions from diverse disciplinary perspectives. We draw from Science and Technology Studies (STS) writ large, including new media studies as well as the philosophy of technoscience and the history of computing.[12] This is not just a joyful exercise of eclecticism, but a thoughtful effort to *compose with*,[13] to bring together diverse insights that permit you to better understand how digital data come to play a pivotal role in security practice. We propose two tropes borrowed from feminist and critical approaches to technoscience – *composting* and *computing*.[14] We argue that both are ways of making sense of, and making sense with, digital data. Composting is about composing data as lively elements, while computing is about composing data as embodied and embodying elements. Both invite us to think of data not as mere output of a single process of datafication, where something is turned 'in[to] a quantified format so it can be tabulated and analyzed'.[15] They rather permit us to think of data in their *becoming something*: a thing whose materiality, meaning and productivity should be investigated in a situated manner. They make us follow 'quasi-objects' characterised by their being at the same time *specific* and *relational*,[16] rather than assuming them as immaterial and representational. Because – as Ikeda's artworks and a growing scientific literature teach us – the materiality, meaning, and productivity of data change across diverse practices.[17]

Our experimental composition is a response to Claudia Aradau's and Tobias Blanke's suggestion that 'data needs to be approached as an object of inquiry rather than subsumed to knowledge'.[18] We argue that a multisensorial approach proves helpful in such an endeavour. As Ikeda's installations remind us, sound and listening – and not only visual machines, graphs, and images – are essential elements of our relation to digital worlds. And, in fact,

---

[12]Defining the appropriate boundaries of STS is probably as difficult as it is useless, since STS is a 'dynamic interdisciplinary field' that is 'extraordinarily diverse and innovative in its approaches'; see Sergio Sismondo, *An Introduction to Science and Technology Studies*, 2nd edn (West Sussex: Wiley Blackwell, 2010), p. vii. It is often difficult to separate STS from new media studies, philosophy of technoscience, or the history of computing. Rather than getting lost in a debate about disciplinary, subdisciplinary, and interdisciplinary labels, we opt for the more open-ended definition of STS writ large.

[13]As Bruno Latour notes, '[e]ven though the word "composition" is a bit too long and windy, what is nice is that it underlines that things have to be put together (Latin *componere*) while retaining their heterogeneity.' See Bruno Latour, 'An attempt at a "compositionist manifesto"', *New Literary History*, 41:3 (2010), pp. 473–4, emphasis in original. Sharing a similar ethos, Isabelle Stengers argues that composing with diverse elements compels us to think with them, that is, to think otherwise; see Isabelle Stengers and Laurent de Sutter, 'Une pratique cosmopolitique du droit est-elle possible?', *Cosmopolitiques*, 8 (2004), p. 15; Serge Gutwirth, 'Composer avec du droit, des sciences et le mode technique: une exploration', in Daniel Le Métayer (ed.), *Les technologies de l'information au service des droits* (Bruxelles: Bruylant, 2010), pp. 24–42.

[14]Notably, Donna Haraway, *Staying with the Trouble: Making Kin in the Chthulucene* (Durham: Duke University Press, 2016); and Wendy H. K. Chun, *Programmed Visions: Software and Memory* (Cambridge, MA: MIT Press, 2011).

[15]Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Eamon Dolan, 2013), p. 78.

[16]Michel Serres, *The Parasite* (Minneapolis: University of Minneapolis Press, 1982), p. 230.

[17]Daniel Rosenberg, 'Data before the fact', in Lisa Gitelman (ed.), *'Raw Data' is an Oxymoron* (Cambridge, MA: MIT Press, 2013), pp. 15–40; Orit Halpern, *Beautiful Data: A History of Vision and Reason since 1945* (Durham, NC: Duke University Press, 2014); Christine L. Borgman, *Big Data, Little Data, No Data* (Cambridge, MA: MIT Press, 2015); Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi, 'Data colonialism through accumulation by dispossession', *Environment and Planning D*, 34:6 (2016), pp. 990–1006; Paul Dourish and Edgar Gómez Cruz, 'Datafication and data fiction', *Big Data & Society*, 5:2 (2018), pp. 1–10.

[18]Aradau and Blanke, 'The (big) data-security assemblage', p. 9.

they have informed and continue to affect security practice and computing.[19] In this article, we pay special attention to what sonic experiences of the digital can teach us about security compositions: how they can help us to deepen an exploration of data as something, and as something becoming part of a security something (else). We suggest that our tropes are well suited for this experimentation because they foreground practices of *togetherness,* as signalled by the common prefix *com* of *com*posting and *com*puting. Here, togetherness is not simply the result of a composition, that is, a tightened fabric of fixed relations, but it is the very process of composing, which is an eminently political and unstable activity of becoming. By attending to togetherness, we can explore security practice as it were not a matter of clear-cut assemblages, but rather a constant, composite, and non-linear attempt to 'make something with something'.[20]

   This contribution comes along, in itself, as a composition. A series of brief accounts of artistic data compositions come to punctuate, interrupt, and inform what would be, otherwise, quite a traditional structure. These paragraphs – like the one opening this introduction – are formatted in italics. One of these accounts is accompanied by an image taken by a photographer during Ikeda's exhibition at the Eye Filmmuseum Amsterdam (September to December 2018).[21] While the accounts do not directly speak about security practice, they mirror embodied experiences of digital data that are valuable for CSS because they run counter to a certain 'visualism' of social sciences and humanities.[22] In the next section, we discuss how critical security scholars approach (or not) digital data in their work. In conversation and in response to this literature, we then propose moving towards a critical study of security compositions. We sample the diverse smorgasbord of STS rather than gorging on one (fashionable) concept or author as the ultimate fix to CSS' shortcomings. In this spirit, we introduce some terminological reflections on the tropes we propose – composting and computing. Even though our contribution is chiefly of a conceptual nature, we also use each trope to unpack a given security practice. We retrace how passenger data become composting material for European law enforcement authorities. And we explore how asylum seekers' voices are turned into data and then computed by governmental agencies to assess the (un)trustworthiness of migrants' claims. Based on these inputs, we turn our ear to contemporary composers. We walk into a multisensorial exploration of technology and security – where data as sound and noise come to trouble often too silent surveillance practices. Eventually, these steps permit us to address, in the outro, the question of how to grasp security data practice, and thus what it means to live in data-informed worlds.

---

[19]Christian Kassung, 'Falling darts, a lost submarine, and a blind man: Notes on the media history of navigating through noise', in Nathanja Van Dijk et al. (eds), *Navigating Noise* (Berlin: Verlag der Buchhandlung Walther König, 2017), p. 77; David Link, *Archaeology of Algorithmic Artefacts* (Minneapolis: University of Minnesota Press, 2016), pp. 69–ff.

[20]Guattari in Guattari and Zahm, 'On contemporary art', p. 45.

[21]Permission for the use of these images has been kindly granted by the Eye Filmmuseum, Amsterdam (Photos by Studio Hans Wilschut).

[22]Don Ihde speaks of 'visualism' to question the dominance of vision and of visuality in shaping how we think about the world, especially when we do so in a scientific manner. See Don Ihde, *Listening and Voice* (Albany: SUNY Press, 2007 [orig. pub. 1976]), pp. 6–ff. Recently, CSS scholars have voiced calls for a renewed attention to non-visual (in)security practices and to more embodied approaches to speech; see Michelle Weitzel, 'Audializing migrant bodies: Sound and security at the border', *Security Dialogue*, 49:6 (2018), pp. 421–37; and Xavier Guillaume, 'How to do things with silence: Rethinking the centrality of speech to the securitization framework', *Security Dialogue*, 49:6 (2018), pp. 476–92.

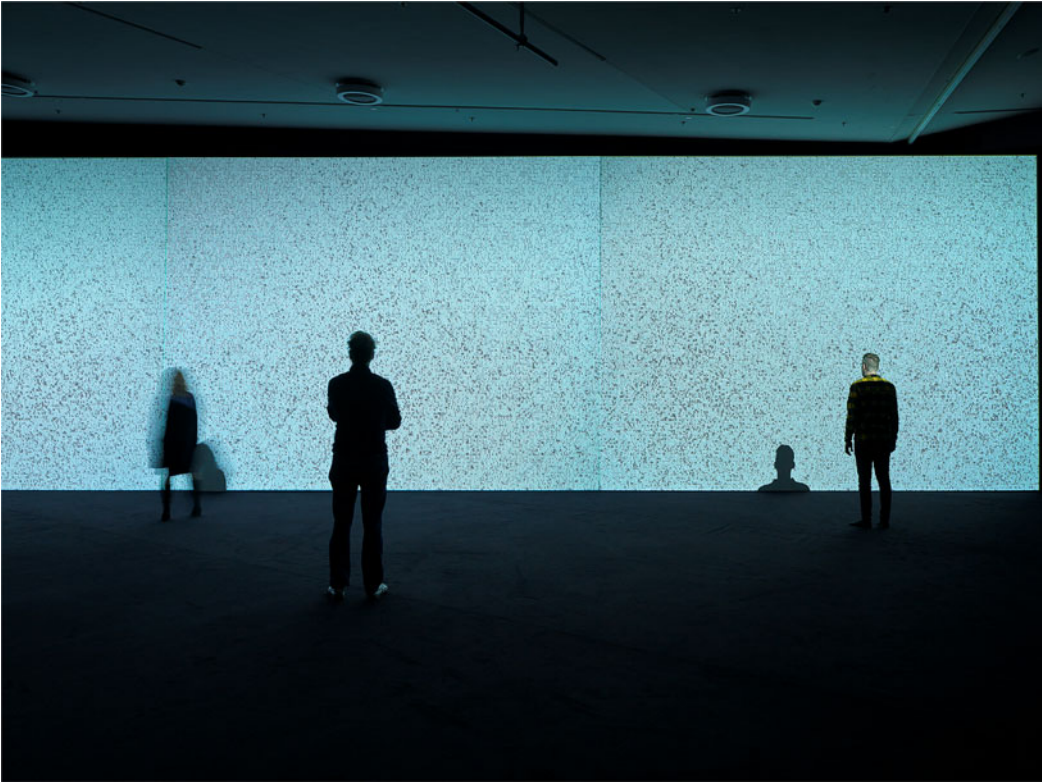## Digital data in Critical Security Studies

Figure 1. 'Ryoji Ikeda', September to December 2018, Eye Filmmuseum, Amsterdam. Photo: Studio Hans Wilschut.

What are we looking at when we look at digital data? Powerful projectors are beaming white light against an enormous black wall. The same light turns people into shadows and silhouettes, while exposing the museum's infrastructure. Ultimately, the above picture (Figure 1) *makes it nearly impossible to firmly say what we are actually looking at. Alphanumerical characters, bits, people, shadows, profiles, infrastructure? Besides, the digital file on which the image is stored is not formatted to convey the constant noise, the constant pulse in our eardrums.*

Well before the so-called Snowden revelations,[23] CSS scholars had already engaged with security technologies. In particular, critical researchers were among the first to look at how data-driven systems (re)shape the security governance of the international. They cast a light on the growing deployment of biometric controls, and the multiplication of databases as security mechanisms.[24] Focusing on data analytics, their work now unpacks the forms of knowledge

---

[23]Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob B. J. Walker, 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology*, 8:2 (2014), pp. 121–44; David Lyon, 'Surveillance, Snowden, and big data', *Big Data & Society*, 1:2 (2014), pp. 1–13.

[24]Among others: Amoore, 'Biometric borders'; Didier Bigo and Elspeth Guild (eds), *Controlling Frontiers: Free Movement Into and Within Europe* (Aldershot: Ashgate, 2005); Dennis Broeders, 'The new digital borders of Europe', *International Sociology*, 22:1 (2007), pp. 71–92; Benjamin J. Muller, *Security, Risk and the Biometric State* (New York: Routledge, 2010); Polly Pallister-Wilkins, 'How walls do work: Security barriers as devices of interruption and data capture', *Security Dialogue*, 47:2 (2016), pp. 151–64.

that underpin data-led security practices,[25] and investigates the institutional relations that organise sociotechnical assemblages.[26] Often in conversation with Surveillance Studies,[27] critical security scholars have built a solid literature on the many ways in which governmental and private actors use digital data to govern populations. However, what is often missing in these accounts is proper attention to the diverse roles of (digital) data. Data are implicitly understood as if they were just 'out there', naturally available in great quantity, as an obvious by-product of our digital age. Even when critical scholars think of data as the data-doubles of individuals,[28] the tendency is to present them in rather immaterial terms. For instance, the digital format of data is considered as a mere facilitator for the spread of algorithmic governance. It is only seldom thought of as a crucial site of bio- and disciplinary politics, that is, where a 'whole range of decisions that affect the look, feel, experience, and workings of a medium' happen, and where 'a set of rules according to which a technology can operate' are decided and tentatively imposed upon others.[29] In other words, in most CSS literature, data are not something to be problematised and accounted for. They are assumed as a given, an instrumental entity that just makes the work of those who govern easier, and that facilitates exchange and cooperation among security actors.

Increasingly, however, this view about data and security practice is evolving. For instance, Evelyn Ruppert et al. state 'that data has a performative power that is resignifying political life'.[30] Their perspective opens up a more historical and sociological approach of datafication processes. Their main focus is on the social dynamics that give meaning to data practices. As they note, 'data is not an already given artefact that exists … but an object of investment … that is produced by the competitive struggles of professionals who claim stakes in its meaning and functioning'.[31] There is great value in this kind of approach. For instance, Didier Bigo's study of data analysts working in security agencies shows how the very accumulation of data becomes a powerful justification to shape any further vision of European security cooperation.[32] Moreover, research carried out in the same vein casts a light on how diverse security agencies rely on data as valuable capital to establish transnational and public-private relations,[33] and to govern at a distance.[34]

Researchers focusing on pre-emptive security unpack an important facet of data politics. Their studies show how the present and the past become data sources for visualising a 'speculative' future, which becomes the informational ground on which security decisions about action can be taken today.[35] These works highlight the crisis of the representational model through which

---

[25]Louise Amoore and Volha Piotukh, 'Life beyond big data: Governing with little analytics', *Economy and Society*, 44:3 (2015), pp. 341–66; Louise Amoore and Marieke De Goede, 'Governance, risk and dataveillance in the war on terror', *Crime, Law & Social Change*, 43:2–3 (2005), pp. 149–73.

[26]Julien Jeandesboz, 'Justifying control: EU border security and the shifting boundaries of political arrangement', in Raphael Bossong and Helena Carrapico (eds), *EU Borders and Shifting Internal Security* (Heidelberg: Springer, 2016), pp. 221–38; Emmanuel-Pierre Guittet and Julien Jeandesboz, 'Security technologies', in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 229–39; Govert Valkenburg and Irma Van Der Ploeg, 'Materialities between security and privacy', *Security Dialogue*, 46:4 (2015), pp. 326–44.

[27]David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London: Routledge, 2003); Didier Bigo, 'Security, exception, ban and surveillance', in David Lyon (ed.), *Theorizing Surveillance* (Devon: Willian Publishing, 2006), pp. 46–68; Elia Zureik and Mark Salter (eds), *Global Surveillance and Policing: Borders, Security, Identity* (Portland: Willan, 2005).

[28]Kevin Haggerty and Richard Ericson, 'The surveillant assemblage', *British Journal of Sociology*, 51:4 (2000), pp. 605–22.

[29]Jonathan Sterne, *MP3: The Meaning of a Format* (Durham: Duke University Press, 2012), p. 7.

[30]Evelyn Ruppert, Engin Isin, and Didier Bigo, 'Data politics', *Big Data & Society*, 4:2 (2017), p. 2.

[31]Ibid., p. 5.

[32]Didier Bigo, 'The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/ police – database analysts', *Security Dialogue*, 45:3 (2014), pp. 209–25.

[33]Didier Bigo, 'International flows, political order and social change', *Global Crime*, 18:3 (2017), pp. 303–21.

[34]Bigo and Guild, *Controlling Frontiers*.

[35]Marieke de Goede, *Speculative Security* (Minneapolis: University of Minnesota Press, 2012).

we generally understand data. What security actors work with, according to Louise Amoore, is mainly a 'data derivative [that] is not centred on who we are, nor even on what our data says about us, but on what can be imagined and inferred about who we might be – on our very proclivities and potentialities'.[36] In other words, the power of data does not lie in their conveying information about us or about a given state of existing affairs. Data – and in particular *digital* data – have value for security actors because they are *composable* into what Amoore calls a 'mosaic', that is, the backdrop justification of a security decision that aims to prevent a future state of affairs from coming into being.[37] Her work highlights how this post-representational use of data in security practice is highly problematic. First of all, it is difficult for those who are governed to challenge a mosaic whose tiles are often shrouded by secrecy, and whose selection criteria are not disclosed by security actors.[38] But it is also problematic for some security practitioners. As Amoore notes, '[t]he "real time decision" … is simply read off from the derivative – replacing the agonism and radical uncertainty of decision and placing responsibility in the realm of response.'[39] This form of automation – or 'decision support' system, in the official discourse of some institutions[40] – redefines the role and power of some security actors. For instance, it disempowers those that have no say in what is left to 'real decision[s]', that is, the seemingly mundane adjustments of a security composition's parameters.[41] In sum, this literature foregrounds the necessity to take seriously the diverse ways in which data become part of a security composition, and how they affect the other elements of the same composition.

On their own, the two described strands of the CSS literature fail to provide a fully useful way to grasp digital security compositions. The former approach shows how data and databases are now established and widely recognised tools for doing security. The latter brings us closer to the material and cognitive inner workings at play in data-driven security practice. Obviously, the common concerns at the core of these literatures are the evolving practices of governing through (digital) data. Yet, these studies tend to overlook the other side of the coin – the governing of data themselves. Sociological approaches are chiefly concerned with a focus on how humans and human institutions – be they border control agents, or security agencies – use their access to data (bases) to act upon other humans or other human institutions. Data and databases are, once established, considered the somewhat constant elements of a security assemblage. Sociomaterial approaches engage more closely with specific technologies, in particular with more or less advanced data analytics, and question how data practices coorganise new ways of doing security and thinking the political. But these works, albeit implicitly, foster a problematic worldview of data compositions. Their emphasis on the role of risk calculation and algorithms presupposes that 'data is passive and algorithm is active', while, in actual fact, 'the passive/active distinction is not quite accurate since data does not just exist – it has to be generated'.[42] And – as we suggest – they not only have to be generated, but also composted, computed and ultimately governed.

Towards a critical study of digital security compositions

Yasunao Tone is, like Ikeda, a Japanese artist working on experimental approaches to music and sound. He has a special interest in (dis)information and noise – noise here both in the sense of

---

[36]Amoore, 'Data derivatives', p. 28.

[37]Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013), pp. 84–ff.

[38]Ibid., p. 85.

[39]Amoore, 'Data derivatives', p. 38.

[40]US DHS Privacy Office, *Privacy Impact Assessment Update for the Automated Targeting System* (Washington: United States Department of Homeland Security, 2017), p. 1.

[41]Amoore, 'Data derivatives', p. 38.

[42]Lev Manovich, *The Language of New Media* (Cambridge, MA: MIT Press, 2002), p. 224.

potentially meaningless data, and of sound.[43] *He often plays with code, images, text, and, most importantly, the translations between them, that is, how something becomes something else.*[44] *Tone has explored the digital by playing with altered CDs, that is, CDs submitted to physical deterioration. CDs are attacked, scratched, damaged, decorated with tape, and then played, generating music based on glitch and noise. The altering of the discs must, however, be limited. CD players are indeed designed to deal with a degree of problems, and sonically compensate for instance some minor scratching. Beyond a certain degree of problems, however, CD players will regard the CD as unfit for playing, and just stop. The artist can thus play with the system only to the extent that the system does not interpret the situation as excessively problematic.*[45]

Our contribution is an invitation to broaden the scope of CSS with regard to data security compositions, by exploring the ways in which data are played with in such compositions. Against the backdrop of the CSS literature discussed above, we suggest following how data become something with which something else can be done. Our previous research[46] and current fieldwork[47] invite us to take seriously the fact that several actors consider data as they were both a solution *and* a problem for security practice.[48] Not only does distinguishing noise from signal remain problematic despite the much-trumpeted breakthroughs in machine learning or artificial intelligence, but there are also manifold actors – be they human institutions, legislative instruments, or technical infrastructures – that are busy generating, storing, integrating, curating, and protecting data.[49] In other words, governing data creates the condition of possibility to govern people and things.

Our insight is further supported by Matthias Leese's empirical work on 'standards and standardization', which shows the potential of unpacking 'the choices within standardization' for specific data and data-driven technologies.[50] Similarly, Mareile Kaufmann et al. argue that patterns for predictive policing are to be understood as 'matter[s] of concern'.[51] They are not linear descriptions of an (in) security reality 'out there', but 'depend on specific algorithms and databases that bring them into being, as well as on decisions whether a pattern is considered meaningful in the specific context of predictive policing'.[52] This article contributes to this emerging CSS literature by foregrounding how digital data matter *even before* they come to matter in more traditional security terms;[53] in

[43]Yasunao Tone, *Noise Media Language* (Berlin: Errant Bodies Press, 2007), p. 85.

[44]Brandon Labelle, *Background Noise: Perspectives on Sound Art*, 2nd edn (London: Bloomsbury, 2015), p. 218.

[45]Christian Marclay and Yasunao Tone, 'Record, CD, analog, digital', in Christoph Cox and Daniel Warner (eds), *Audio Culture: Readings in Modern Music* (London: Bloomsbury, 2017), p. 344.

[46]Bellanova and González Fuster, 'Politics of disappearance'; Rocco Bellanova, 'Digital, politics, and algorithms: Governing digital data through the lens of data protection', *European Journal of Social Theory*, 20:3 (2017), pp. 329–47; Gloria González Fuster, 'Transparency as translation in data protection', in Emre Bayamiloglu, Irina Baraliuc, Liisa Janssens, and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam: Amsterdam University Press, 2018), pp. 52–5.

[47]For example, one of us is currently investigating how EU institutions work towards further facilitating and speeding up access to data across national borders and sectors, while the other is studying how European security actors are coping with large amounts of data, including issues concerning data architecture and integration as well as data curation and storage.

[48]In Foucauldian terms, this means that digital data – being considered key to the functioning of calculative devices – have become a *problematic of government*; see Paul Rabinow and Michel Foucault, 'Polemics, politics and problematizations: an interview with Michel Foucault', in Paul Rabinow (ed.), *The Foucault Reader* (New York: Pantheon Books, 1984 [orig. pub. 1983]), pp. 381–90.

[49]The ongoing European debates surrounding the so-called 'principle of interoperability' are a good example of these efforts. General Secretariat of the Council, *Final Report by the High Level Expert Group on Information Systems and Interoperability (HLEG)* (Brussels: Council of the European Union, 2017). Interoperability projects are often a source of conflicts and a site of powers redistribution; see Ann-Sofie Hellberg and Åke Grönlund, 'Conflicts in implementing interoperability: Re-operationalizing basic values', *Government Information Quarterly*, 30:2 (2013), pp. 154–62.

[50]Matthias Leese, 'Standardizing security: the business case politics of borders', *Mobilities*, 13:2 (2018), p. 262.

[51]Kaufmann, Egbert, and Leese, 'Predictive policing and the politics of patterns', p. 675.

[52]Ibid.

[53]Nathaniel O'Grady, 'Data, interface, security', *Geoforum*, 64 (2015), pp. 130–7; Marieke de Goede, 'The chain of security', *Review of International Studies*, 44:1 (2018), pp. 24–42; Georgios Glouftsios, 'Governing circulation through technology within EU border security practice-networks', *Mobilities*, 13:2 (2018), pp. 185–99.

other words, even before they become 'data derivatives', a tile of a security 'mosaic', or a pattern to be visualised. For instance, Tone's artwork emphasises the importance of the material support on which data are stored. Taking care of appropriate storage conditions is essential for data to become something through(out) their life cycles.[54]

In the spirit of composition promoted by this Special Issue,[55] we embark on a conversation with multiple works. We draw from diverse disciplines – STS writ large, but also diverse art forms, especially sound and music. While CSS has punctually engaged with leading STS authors and core concepts,[56] we believe that there is still a great untapped potential in such a vibrant and diverse literature. This is where our tropes of composting and computing come from. And it is from artists and art critics that we learn to attend to the sound – to look at data beyond visuality. Rather than proposing one more (sonic) turn to CSS, we bring STS scholarship and arts to bear on a critical study of digital security compositions.[57] By attempting to recompose them into our contribution, we wish to challenge our own (disciplinary) understanding of digital data. And this, we humbly suggest, is already a way to unpack and question digital security compositions.

The composting trope

Back to Ikeda's exhibition. These sounds, these lights, are the by-product of datasets generated for other purposes. As is often the case, Ikeda has mainly used 'scientific datasets'.[58] *Right here, right now, they give way to unforeseen images and sounds, to a new world. And there are a lot of data surrounding you. An avalanche of numbers turning into their own cartography. Lines of different lengths that roll through a giant screen. Diagrams emerge out of the mess, pointers move up and down, left and right – they insist on a specific point. The images change continuously. Even those standing still become something else. If you turn your head quickly, your peripheral vision captures a multitude of colours out of the intensely white beam of the lamp. The camera of your smartphone will only record these changing colours. It is unable to process the light pulses the same way as you are sensing them. And there is this constant (data) noise.*

Philosopher of technoscience Donna Haraway often uses the trope of *compost*.[59] In her work, compost functions both as a verb and a noun. She explains that: 'I work with string figures as a theoretical trope, a way to think with a host of companions in sympoietic threading, felting, tangling, tracking, and sorting. I work with and in SF [science fiction] as material-semiotic composting, as theory in the mud, as muddle.'[60] Composting can be thus understood as a theoretical trope, but one where the concept – if we wish to call it a concept – is not purified from its everydayness. In other words, composting only works well as a trope when we first relate to the mundane practice of compost.

Compost is 'decayed organic material used as a fertilizer for growing plants'.[61] By extension, it is 'a mixture of compost or similar material with loam soil used as a growing medium'.[62] As a verb, to compost is both to 'make (vegetable matter or manure) into compost' and to 'treat

---

[54]Matthew Kirschenbaum, 'Extreme inscription: Towards a grammatology of the hard drive', *TEXT Technology*, 13:2 (2004), pp. 91–125.

[55]Jonathan Luke Austin, 'Security compositions', *European Journal of International Security*, 4:3 (2019), this Special Issue.

[56]Among many, see Claudia Aradau, 'Security that matters', *Security Dialogue*, 41:5 (2010), pp. 491–514; Jacqueline Best and William Walters, '"Actor-network theory" and international relationality', *International Political Sociology*, 7:3 (2013), pp. 332–4; Thierry Balzacq and Myriam Dunn Cavelty, 'A theory of actor-network for cyber-security', *European Journal of International Security*, 1:2 (2016), pp. 176–98.

[57]As such, our approach resonates with the viewpoint of those involved in the International Studies Association section on Science, Technology, and Arts in International Relations (STAIR); J. P. Singh, Madeline Carr, and Renee Marlin-Bennett (eds), *Science, Technology, and Art in International Relations* (London: Routledge, 2019).

[58]Eye Filmmuseum, 'Ryoji Ikeda', exhibition brochure.

[59]Haraway, *Staying with the Trouble*.

[60]Ibid., p. 31.

[61]See Oxford English Dictionary.

[62]Ibid.

(soil) with compost'.[63] Not surprisingly, the term shares the same etymological roots as composition. According to the dictionary, both terms can be traced back to the Latin verb *componere*, meaning 'put together'.[64] Starting with the mundane of composting may be promising, both for gardeners and for theorists. The *Practical Handbook of Compost Engineering* notes that '[t]here is no universally accepted definition of composting', but that, in 'practical' terms, 'composting is a form of waste stabilisation, but one that requires special conditions of moisture and aeration to produce thermophilic temperatures'.[65] Philosophers Sebastian Abrahamsson and Filippo Bertoni seem to agree, as they argue that '[v]ermicomposting is complex: the coexistence of heterogeneous and disparate processes and entities may bring about problems.'[66] For composting to succeed, the steering of the work of many is needed, and an understanding of what each thing may specifically contribute is often essential. As Abrahamsson and Bertoni suggest, this opens several questions about the kind of politics that composting triggers.[67] For instance, Haraway's recent work plays with the idea that composting presupposes, or, better put, enacts some forms of composition. Both composition and compost are about doing 'something with something' (to borrow again from Guattari).[68] They are about accepting that there is a state of affairs with something already going on. That there are things already there that may be brought together. Composting and composing are processes. The things that are already there modify what comes to them, and they are modified in the encounter. They are *transformed and transformative* things, undone and enriched by the same process. A piece may be broken to adjust to another. A melody emerges by the juxtaposition of some notes (and silences). As Ikeda's artworks vibrantly show, datasets are recoded and curated, and we may end up developing a better knowledge of our world – even if his datascapes do not convey any information about it.

Composting troubles the somewhat classical questions about who the agent of the action is. Is it the vermicomposter? The worms eating the waste? The waste itself? This trope shows that providing a simple and unequivocal answer may be missing the point. The questions themselves reify a linear model in which there is a unique subject that acts, while everything else becomes the object of that action (a target or a tool). Composting highlights the need to organise the appropriate conditions of participation for discrete elements, that may contribute to the overall action of turning what for some people is waste into food for worms, then soil, and eventually nutrients for plants. In some cases, the conditions facilitating composting rely on the yeast that must be added. This is what we illustrate in the following section, where some digital data are curated to act as compost for speculative security action. In other cases, some data are extracted from larger datasets, enriched with further meta-data and stored away – to be cross-matched when new information is received and mobilised in support of an investigation. In sum, rather than striving to locate the ultimate agent, we aim at understanding how data as something are inscribed into a rationale of governing – what has to be put in place to make the compost produce its 'productive juice'.

In the following section, we suggest thinking Big Data security from the vantage point of the composting trope. This means to explore Big Data's expectations and anxieties about the increase of noise in a situated manner. According to Rob Kitchin, 'Big Data is characterized by being generated continuously, seeking to be exhaustive and fine-grained in scope, and flexible and scalable in its production.'[69] This also implies the 'challenge of analysing' these data, that is, 'coping with abundance, exhaustivity, and variety, timeliness and dynamism, messiness and uncertainty, high relationality, and the fact that much of what is generated has no specific question in mind or is a by-product

---

[63]Ibid.

[64]Ibid.

[65]Roger T. Haug, *The Practical Handbook of Compost Engineering* (Bocan Raton: Lewis Publishers, 1993), p. 1.

[66]Sebastian Abrahamsson and Filippo Bertoni, 'Compost politics: Experimenting with togetherness in vermicomposting', *Environmental Humanities*, 4:1 (2014), p. 142.

[67]Ibid., pp. 142–3.

[68]Guattari in Guattari and Zahm, 'On contemporary art', p. 45.

[69]Rob Kitchin, 'Big data, new epistemologies and paradigm shifts', *Big Data & Society*, 1:1 (2014), p. 2.

of another activity'.[70] In other words, too many digital data are constantly being produced, stored, and processed. This simultaneously invites and requires the deployment of appropriate computing power, storing capacities, and knowledge practices.[71] The assumption underlying big data practices is that there must be a great potential in this ever-growing mass of data. Still, avoiding getting lost in the translation of too many data sources is a major issue for security actors.

Security as recycling data

Composting digital data, rather than avoiding ingesting them in first instance, is the main solution adopted by the European legislator in the face of data proliferation. Take the Passenger Name Record (PNR) Directive, which is a massive scheme for air passenger surveillance.[72] Adopted in 2016 by the European Union (EU), it requires all air carriers to transfer passenger information to national law enforcement authorities, whenever a commercial aeroplane flies between a EU Member State and a third country.[73] All passengers are filtered through the checking of their PNR, even if only a few will be stopped or denied boarding. As such, the PNR system embodies the ambition of many governmental actors and private companies arguing that data-driven technologies eventually permit the control of circulation without hampering flows.[74] PNRs are essential for the continuous working of the commercial air sector as we now know it; their circulation greatly facilitates air travel.[75] The PNR Directive creates another cycle of use for these pre-existing data. Here PNRs are recycled in the sense that they are routed not only to commercial actors but also to security authorities, the Passenger Information Units. These new law enforcement units are responsible for storing, processing, and exchanging PNRs. They continuously receive vast amounts of personal data, and have to analyse this information for a purpose different than the original one, for example counterterrorism or organised crime prevention. One could attempt to picture this as a perpetual reinvention of life for data, but only, we suggest, by including the fact that such renewal implies processes of coming apart, breaking down, and decay.

The organisation of the novel PNR lifecycle can be aptly understood with the help of the composting trope. For a start, the very creation of an automated system for transferring data from reservation systems to national authorities required the development of a new messaging standard. The system now endorsed by several countries and companies, PNRGOV, was developed by a private-public working group led by the International Air Transport Association (IATA).[76] This recycling step demonstrates that data are both socially *and* materially constructed, and that their construction, curation, and – if necessary – reformatting are necessary to enable security composition. So far, CSS literature has paid too little attention to security actors' organisational efforts underpinning the recycling of data into a security practice. The main focus of critical research has tended to remain the irruption of advanced data analytics and the cohort of private and

---

[70]Ibid., p. 2.

[71]It is a phenomenon akin to the 'avalanche of printed numbers' that hit Western administration in the early nineteenth century. See Ian Hacking, 'Biopower and the avalanche of printed numbers', *Humanities in Society*, 5:3–4 (1982), pp. 279–ff.

[72]European Parliament and Council, 'Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime' (Luxembourg: Official Journal of the European Union, 2016). Cf. in extenso: Lena Ulbricht, 'When big data meet securitization: Algorithmic regulation with Passenger Name Records', *European Journal for Security Research*, 3:2 (2018), pp. 139–61.

[73]PNR are commercial datasets inscribing a wide range of information, from the name of the passenger and the method of payment used to buy the ticket, to frequent flyer numbers and travel itineraries.

[74]Leese, 'The new profiling'.

[75]Martin Dodge and Rob Kitchin, 'Flying through code/space: the real virtuality of air travel', *Environment and Planning A*, 36:2 (2004), pp. 195–211.

[76]See {https://www.iata.org/publications/store/Pages/passenger-data-exchange.aspx} accessed 15 October 2018.

public actors promoting and adopting them for security purposes.[77] Yet, the governmental ambition to let data speak by themselves requires much more than the data in and of themselves. It presupposes the technical ability to receive and handle data from various sources, as well as the adequate computing infrastructure to process them and the statistical expertise to make (some) sense of them. The importance of these 'feasibility' requirements is becoming evident to those authorities that want to compost PNR for their security compositions.[78]

Big data security practice promises to connect the dots. Composting illustrates how this ambition is supposed to function in practice. According to the European legislator, the added value of a PNR-based surveillance system is the ability to identify 'unknown suspects',[79] that is, those travellers that are not (yet) sought by law enforcement authorities. In the text of the PNR Directive, this practice is called risk assessment, and it requires two forms of dot connection. First, a series of profiles should be drawn. Then, a link between a profile and an actual traveller should be established. To sketch a profile, not only external intelligence is to be used, but also the very PNR data stored by the Passenger Information Units.[80] These datasets are thus expected to act as reactive agents, to complement the intelligence coming from outside the PNR database. In this sense, the storage of PNRs for a long period after their initial 'depersonalisation'[81] (for a total of five years) is motivated by the expectation that this extended lifecycle may permit their further recycling. In turn, this would give way to better knowledge generation as if (somewhat decayed) PNRs were compost in a dynamic data-bin.

But composting does not only happen when security agencies want to deploy 'predictive' algorithms or machine learning systems. It is also at play in more classic investigative work, especially when this involves dealing with potentially overwhelming sources of data. Take, for example, existing European approaches to terrorism content posted on Internet platforms. At present, the EU Internet Referral Unit flags '"jihadist" terrorist online propaganda' on social media, asking for its removal.[82] At the same time, it stores this material in an 'electronic reference library' that 'contains, *in a structured way*, original statements, publications, videos and audios produced by terrorist groups or their supporters'.[83] The main goal of this composting operation is to facilitate future investigations. Here, digital data can become a security something, for example the potential pieces of a future 'mosaic'.[84] However, this happens only when data have been properly recycled, that is, stored, preserved, and put at the disposal of other actors - such as law enforcement authorities and IT systems.

In sum, thinking about this security practice with the trope of composting offers us some critical vantage points. Composting is a trope and an activity closely related to Haraway's commitment to 'stay with trouble'.[85] This *trouble* is also, as Thierry Hoquet reminds us, an eminently present

---

[77]For instance, Matthias Leese does a great job in unpacking different forms of profiling practices, and in casting a light on the implications of those promoted by the EU PNR project; see Leese, 'The new profiling'. On the role of private companies, especially software houses and consulting firms, see Amoore, *The Politics of Possibility* and Amoore and Piotukh, 'Life beyond big data'.

[78]Despite political momentum and consequent funding, the setting up of the EU PNR scheme remains slow; see {http://www.europarl.europa.eu/doceo/document/E-8-2017-006210-ASW_EN.html?redirect#def4} accessed 15 October 2018. See also U² Consortium, *Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information (and Passenger Name Records), Volume 1: Main Report* (Brussels: European Commission, 2019).

[79]As the PNR Directive states: 'Assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities.' European Parliament and Council, 'Directive (EU) 2016/681', recital 7.

[80]Rocco Bellanova and Denis Duez, 'A different view on the "making" of European security: the EU Passenger Name Record system as a socio-technical assemblage', *European Foreign Affairs Review*, 17:2–1 (2012), pp. 109–24.

[81]The EU PNR Directive states that '[u]pon expiry of a period of six months after the transfer of the PNR data …, all PNR data shall be depersonalised through masking out the … data elements which could serve to identify directly the passenger to whom the PNR data relate.' European Parliament and Council, 'Directive (EU) 2016/681', Article 12(2).

[82]EU Internet Referral Unit, *Transparency Report 2017* (The Hague: Europol, 2018), p. 5.

[83]Ibid., p. 5, emphasis added.

[84]Amoore, *The Politics of Possibility*, p. 84.

[85]Haraway, *Staying with the Trouble*.

situation that should not be avoided even if difficult.[86] Critical security scholars have discussed the deployment of PNRs and similar data-driven systems as a way to dodge the trouble of present, if not imminent, security threats by visualising and mobilising future ones.[87] However, composting invites us to shift attention from the algorithmic ambitions of the system to the diverse ways in which data become something, now and in the future. Similarly to the notion of data derivative, this points towards the need for a better understanding of the temporality of the 'real decision' concerning security action.[88] However, composting insists on understanding data as lively entities – whose lives are to be continuously supported or organised. It thus foregrounds security actors' efforts to continuously ensure the material conditions that enable their (security) composition. This means curating, storing, and protecting data in a way that their security compositions are – in composting jargon – 'stabilized'. The fact that this is not an easy task opens up new research and political avenues. It obliges critical security scholars to resist the idea of a security system as a black box, or as a practice that will ever become black-boxed. It also offers a political grip on the security practice itself, inviting scholars to stay with the trouble of studying security actors' troubles with digital data. It multiplies questions about what is to be considered a *good* data composition, thus supplementing those raised during the legislative process. Grasping how digital security compositions work in practice might require that *we stop focusing on opening the black box*. Instead we may want to take the time to rip it up, shake its components, and pay attention to how that actually sounds. Ikeda's compositions resonate vibrantly in this endeavour.

The computing trope

Let's go back again to Ikeda's artwork. Stepping into Ikeda's installation may be overwhelming. You are invited to leave the quest for a univocal meaning outside the door. The titles of the installations are only on the brochure. The only signposts are the white lines on the wall, just after the entrance. They tell you that '[Ikeda] develops his computer programs and algorithms that generate the images and sounds for his compositions.' No composition here saw the light of day without some form of computing. Compared to your everyday experience of the digital, whose inner workings become perceivable only when problems occur, you are now face to face with manifestations of computer processing that co-produce extremely bodily experiences, directly targeting your senses. Through constant sound, these experiences generate and sustain a dissonance with your all-too-polished perception of what data are supposed to look or sound like.

In order to achieve a more embodied understanding of digital data, we should take computing seriously. Introducing computing as a trope may sound counterintuitive, especially since the work of CSS on data-driven security already foregrounds algorithms and calculative techniques.[89] However, our inquiry concerns the connections between compost, the *componere* of compositions, and the *computus* behind computers and data. If we accept the idea that *computus* is rooted in the counting of one's fingers (*digitus*), as opposed to the more abstract *calculus*,[90] we are brought back to the need to consider the inherent materiality of digital security compositions. The term *computare* is, itself, a combination of *com* (together) and *putare* (to settle).[91] That is, it is a term fundamentally about *bringing together*, about *togetherness*. We are confronted with the importance of how, by counting, people and things can be brought together or torn apart.

[86]Thierry Hoquet, 'Pour un compostisme enchanté', *Critique*, 860–861:1–2 (2019), p. 54; see also Jonathan Luke Austin, Rocco Bellanova, and Mareile Kaufmann, 'Doing and mediating critique', *Security Dialogue*, 50:1 (2019), pp. 3–19.

[87]Amoore, 'Data derivatives'; Amoore, *The Politics of Possibility*; Leese, 'The new profiling'.

[88]Amoore, 'Data derivatives', p. 38.

[89]Louise Amoore and Rita Raley, 'Securing with algorithms', *Security Dialogue*, 48:1 (2017), pp. 3–10; Julien Jeandesboz, 'European border policing: EUROSUR, knowledge, calculation', *Global Crime*, 18:3 (2017), pp. 256–85.

[90]Mario Aloisio, 'The calculation of Easter Day, and the origin and use of the word computer', *IEEE Annals of the History of Computing*, 26:3 (2004), p. 42.

[91]Ibid.

The birth of modern computing is deeply rooted in security. Most notable technological advances in the field were triggered by codebreaking efforts, as well as ballistics calculations, before, during and after the Second World War.[92] Computers were initially persons (most often women) responsible for calculation – 'hidden figures' (to borrow from the title of a Hollywood movie)[93] in a complex composition of human and non-human resources that made computing possible. Digital data were only progressively developed as actionable (that is, computable) and storable (and thus reusable) elements, as well as outputs of computing. In this sense, the history of computing does not only retrace the abstract models through which computer designers imagine the world and its politics,[94] but also highlights the material practices through which computers relate, and thus meddles in its world and politics.[95]

The fact that computers compute is however more than a tautology. First, it reminds us that much of the work that computers do is different from what they generally pretend to be doing. It is as if it was better to keep computing far from our sight, although traces of such computing might be heard in the noise produced by some machines – typically dysfunctional, overheating, potentially about-to-die devices. For instance, Wendy Chun notes that '[w]hen the computer does let us "see" what we cannot normally see, or even when it acts like a transparent medium through video chat, it does not simply relay what is on the other side: it computes.'[96] In other words, computers crunch things out there as if they are something else than what they supposedly are – not images or sound, but very material data – be they punch cards, 'variations of magnetic field, voltages, or pulses of light'.[97] And then they spit out further data that can become something else: images or sound. With the diffusion of computers, attention for this passage is often lost. As Chun argues, '[i]n order to become transparent, the fact that computers always *generate* text and images rather than merely represent or reproduce what exists elsewhere must be forgotten.'[98] This is an important reminder of the risk of missing the sites of computing politics. In fact, even critical discourse around data processing is eager to embrace visual similes; it is typically all about transparency and opening the black box.[99] Chun further argues that '[t]he current prominence of transparency in product design and in political and scholarly discourse is a compensatory gesture.'[100] If anything, taking the material practice of computing seriously invites us to resist visual and political shortcuts by retracing its embeddedness in the fabric of security.[101]

Second, computing presupposes some forms of programming. The history of computing shows how material and compositional programming can be. Again, Chun reminds us that: '[a]s computers became machines, programmers became human and programming became functionally equivalent to the process of "setting up" the ENIAC [Electronic Numerical Integrator and Computer]-the physical act of wiring the machine for a particular problem.'[102] As Michael S. Mahoney, historian of computing, notes: '[t]he computer is not one thing … and the same

[92]Paul E. Ceruzzi, *Computing: A Concise History* (Cambridge, MA: MIT Press, 2012).

[93]Theodore Melfi (dir.), *Hidden Figures* (United States: 20th Century Fox, 2016).

[94]Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996); Andrew Pickering, *The Cybernetic Brain* (Chicago: The University of Chicago Press, 2010).

[95]Paul E. Ceruzzi, *A History of Modern Computing*, 2nd edn (Cambridge, MA: MIT Press, 2003); Katherine N. Hayles, *My Mother Was a Computer* (Chicago: University of Chicago Press, 2005).

[96]Chun, *Programmed Visions*, p. 17.

[97]Jean-François Blanchette, 'A material history of bits', *Journal of the American Society for Information Science and Technology*, 62:6 (2011), p. 1042.

[98]Chun, *Programmed Visions*, p. 17, emphasis in original.

[99]Danielle Keats Citron and Frank Pasquale, 'The scored society: Due process for automated predictions', *Washington Law Review*, 89:1 (2014), pp. 1–33; Frank Pasquale, *The Black Box Society* (Cambridge, MA: Harvard University Press, 2015).

[100]Chun, *Programmed Visions*, p. 17.

[101]Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability', *New Media & Society*, 20:3 (2018), pp. 973–89.

[102]Wendy H. K. Chun, 'Programmability', in Matthew Fuller (ed.), *Software Studies: A Lexicon* (Cambridge, MA: MIT Press, 2008), p. 225. The ENIAC was a crucial computing project of the early 1940s, which highlights the close connection

holds true of computing.'[103] He then highlights that '[b]etween the mathematics that makes the device theoretically possible and the electronics that makes it practically feasible lies the programming that makes it intellectually, economically, and socially useful.'[104] In this context, it appears necessary to keep questioning our understanding of computing beyond engineering and mathematical accounts, but also beyond visual imagery and imagination, that is, the transparent machine, the black-boxed processing. Until now, not only scholars but also artists have been struggling to find ways to make the data in big data accessible without necessarily focusing on making them visible.[105] It is as if we were all seduced by the visual power of increasingly aesthetically refined design of data visualisation.[106]

If we are to look beyond visuality, we may want to examine how sound and noise inform information technologies as we know and experience them. Historically, computing emerged by accompanying the interception of sound. In 1943, the first British programmable electronic computer was used to process data (about German communications) collected by wireless intercept operators – women, predominantly, who listened out for Morse code for hours and transcribed it to be processed by the computer.[107] Sound was thus, technically, the original computing raw material. But it was already turned into specific and embodied data, in this case punched cards. Since then, the intersections between sound and security have been studied from a number of perspectives.[108] However, CSS rarely considers the relations of security and sound with and through data.

Listening to the asylum speakers

'New audibilities' have been addressed in the field of critical forensics, which can be described as being at the crossroads of security studies, art, and architecture.[109] From this perspective, the artist and researcher Lawrence Abu Hamdan has notably studied accent monitoring and the automated determination of origin by audio technologies.[110] These data-driven systems are used to judge the veracity of statements by asylum seekers, which become – in his work – 'asylum speakers'.[111] Automated speech analysis practices build upon older and relatively widespread practices of Linguistic Analysis for the Determination of Origin (LADO), or speech analysis by human experts, that is, analysts and linguists.[112] A 2017 report noted that a majority of European countries relied on language analysis as standard practice, or at least occasionally, to determine probable country and/or

between computing and security. Ceruzzi notes that '[w]ith its 18,000 vacuum tubes, the ENIAC was touted as being able to calculate the trajectory of a shell fired from a cannon faster than the shell itself travelled.' See Ceruzzi, *Computing*, p. 46.

[103]Michael S. Mahoney, 'The history of computing in the history of technology', *Annals of the History of Computing*, 10:2 (1988), p. 116.

[104]Ibid., p. 117.

[105]Claudia Mareis, 'The end of representation: Artistic-creative strategies in dealing with big data', in Sabine Himmelsbach and Claudia Mareis (eds), *Poetics and Politics of Data* (Basel: Christoph Merian Verlag, 2015), pp. 43–61.

[106]For an example of data visualisation meeting trending design aesthetics, see Giorgia Lupi and Stefanie Posavec, *Dear Data* (London: Particular Books, 2016).

[107]Marie Hicks, *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing* (Cambridge, MA: MIT Press, 2018), pp. 28–ff.

[108]See, for example, Suzanne G. Cusick, 'Music as torture/music as weapon', *Trans: Revista Transcultural de Música*, 10 (2006); Steve Goodman, *Sonic Warfare: Sound, Affect, and the Ecology of Fear* (Cambridge, MA: MIT Press, 2010); Roman Vinokur, 'Acoustic noise as a non-lethal weapon', *Sound and Vibration*, October (2004), pp. 19–23; Juliette Volcler, *Le son comme arme: Les usages policiers et militaires du son* (Paris: La Découverte, 2011).

[109]Emily Apter, 'Foreword. Shibboleth: Policing by ear and forensic listening in projects by Lawrence Abu Hamdan', in Lawrence Abu Hamdan, *[Inaudible] A Politics of Listening in 4 Acts* (Berlin: Sternberg Press, 2016), p. 3.

[110]Abu Hamdan, *[Inaudible] A Politics of Listening in 4 Acts*.

[111]Ibid.

[112]These practices are also not deprived of controversy, notably concerning their scientific solidity; see, in this sense, Diana Eades, 'Testing the claims of asylum seekers: the role of language analysis', *Language Assessment Quarterly*, 6:1 (2009), pp. 30–40.

region of origin of applicants for international projection.[113] In 2019, Turkey, in the context of its commitments towards the EU to slow down flows of migrants and refugees, started funding a programme of Technical Assistance for Capacity Building for Effective Nationality Determination,[114] to use language tests to identify the origin of a person in asylum cases, relying on both automated systems and humans. Ultimately, these systems resonate with the Biblical episode about the identification of an enemy's survivors through their pronunciation of the word 'shibboleth'.[115]

'Automatic dialect recognition' is part of the toolbox of the Integrated Identity Management (IDM) programme that the German Federal Office for Migration and Refugees (BAMF) introduced in 2016.[116] German authorities started testing these systems in 2017, and implemented them in 2018.[117] To date, they have expressed their eagerness to further work on dialect recognition together with migration authorities from other European countries.[118] The software aims to 'increase process efficiency in the asylum procedure', together with automatic face recognition and the analysis of mobile data devices.[119] All these data-driven systems are directed towards helping decision-makers make sense of the asylum seekers' data collected during registration – here better understood also in sonic terms. In Germany, the initial deployment of 'automatic language recognition', labelled at the time 'language biometrics', met political and societal reluctance, admittedly because the software lacked accuracy.[120] What the tool embodies, in any case, is a certain way of governing through data that does not even pretend to translate reality. It is unconcerned with what asylum speakers actually say, or, more exactly, it is grounded on the assumption that whatever they might say is not worth being taken into account before the trustworthiness of their belonging is ascertained. Despite the seeming invisibility of the computing process, this assessment is extremely embodied – socially and materially. The computer computes migrants because it hears speech as data, which will enter into a conversation with other people's data – it needs data as compositional elements. It lives on configuring life as made of 'components of composite evidence'.[121] It computes to compose. It transforms individuals into elements of a wider security composition, inside which the data about them potentially undergoes a series of further transformations. For instance, German authorities can process audio records collected during asylum procedures and use them outside the asylum procedure, for example, to establish identity or to identify evidence for purposes of criminal prosecution and threat prevention.[122]

---

[113]European Migration Network (EMN), *EMN Synthesis Report for the EMN Focussed Study 2017: Challenges and Practices for Establishing the Identity of Third-Country Nationals in Migration Procedures* (Brussels: European Commission, 2017). In Sweden, LADO work was initiated within the Swedish Migration Board in the early 1990s, and eventually moved to the private sector; see the Sprakab's website: {http://www.sprakab.se/Q%26A.html} accessed 14 April 2019. See also Verified, *LOID – Linguistic Origin Identification* (Solna: Verified AB, 2011). Swedish companies currently provide services *inter alia* for United Kingdom authorities; see UK Home Office, *Language Analysis Version 21.0* (London: Home Office, 2018).

[114]Supported by the European Commission's DG for International Cooperation and Development.

[115]Michael J. Shapiro, 'Every move you make: Bodies, surveillance, and media', *Social Text*, 23:2 (2005), p. 23.

[116]Federal Office for Migration and Refugees (BAMF), *Digitisation Agenda 2020: Success Stories and Future Digital Projects at the Federal Office for Migration and Refugees (BAMF)*, 3rd updated edn (Nuremberg: Publications office of the Federal Office for Migration and Refugees, 2018), p. 34.

[117]Ibid., p. 35.

[118]Ibid.

[119]Ibid.

[120]EMN, *EMN Synthesis Report for the EMN Focussed Study 2017*, p. 41.

[121]Verified, *AI Project Awarded Research Grant Press Release* (2019), available at: {https://www.mynewsdesk.com/se/verified/pressreleases/ai-project-awarded-research-grant-2477301} accessed 14 April 2019. In this press release, the Swedish company Verified announces having obtained funding for research on the use of artificial intelligence solutions for dialect attribution.

[122]Julian Tangermann, *Documenting and Establishing Identity in the Migration Process, Challenges and Practices in the German Context: Focussed study by the German National Contact Point for the European Migration Network (EMN) – Working Paper 76* (Nuremberg: Federal Office for Migration and Refugees, 2017), p. 43.

The governing of asylum seekers *as asylum speakers* highlights a peculiar composition of security through sound and its turning something into data and data into something else.[123] Automatic language recognition in this context tells us about the limits of the audible, and how security practice marks what is to be played. The introduction of the automated means that for linguistic forensics, seemingly 'objective' datasets are generated and brought together – aimed at countering the fact that procedures would otherwise be 'based largely on the claims made by the asylum-seekers themselves'.[124] Approaching this form of security composition with the trope of computing highlights how it differs from other surveillance practices deployed by security actors. Contrary to fingerprinting, the voice samples are not extracted for establishing, assigning, and then enforcing a univocal identity to individuals.[125] While the voice of the asylum seeker may be considered a bodily feature, once sampled and digitised it rather embodies something else. To borrow from Michelle Weitzel, this form of computing is another way to 'audaliz[e] the body' of the migrant and thus one 'of the ways in which sound is … harnessed by powerful actors in the security sphere'.[126] First of all, asylum seekers' voices materially become a dataset that can be compared with an existing database of already stored and classified voices. The voices-turned-data are treated as a sonic 'immutable mobile',[127] rather than a continuously adjusted performance.[128] With these data structures already in place, and the support of an algorithm, it is supposedly possible to identify not individual identities but statistical anomalies.[129] At the same time, the datafied voice embodies the asylum seeker as a uniquely socialised being: a *speaker* who is supposed to have unique social traits, such as an accent, acquired not because of some biological reasons, but due to their socialisation in a given geographical place – a region where a distinctive dialect is spoken. Their voice, because it is social rather than individual, becomes the first 'clue' to be followed.[130]

We argue that there is both heuristic and political value in mobilising the computing trope when it comes to this kind of security compositions. Thinking about this practice in terms of computing counters the rather disembodied image conveyed by proponents of 'automatic dialect recognition'. It invites researchers to unpack what embodies what, and how. Somewhat paradoxically, the fact that computers do not hear or see as we hear and see, foregrounds questions about the social and cultural assumptions underpinning the idea that asylum seekers – or people in general – have a unique linguistic socialisation.

This is the sound of digital security composition

Ikeda became progressively involved in explorations around data, notably through collaborations with, among others, the German musician Carsten Nicolai, with whom he shares an interest in the duality of the senses.[131] Although often described as a minimalist artist, Ikeda is equally

---

[123]On the datafication on European borders, see, for example, Dennis Broeders and Huub Dijstelbloem, 'The datafication of mobility and migration management', in Irma van der Ploeg and Jason Pridmore (eds), *Digitizing Identities* (London: Routledge, 2016), pp. 242–60; Philippa Metcalfe and Lina Dencik, 'The politics of big borders: Data (in)justice and the governance of refugees', *First Monday*, 24:4 (2019).

[124]BAMF, *Digitisation Agenda 2020*, p. 12.

[125]Charlotte Epstein, 'Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders', *International Political Sociology*, 1:2 (2007), pp. 149–64.

[126]Weitzel, 'Audializing migrant bodies', p. 423.

[127]Bruno Latour, 'Visualization and cognition: Drawing things together', in Henrika Kuklick (ed.), *Knowledge and Society Studies in the Sociology of Culture Past and Present* (Greenwich: Jai Press, 1986), p. 7.

[128]See the criticism about LADO in Natalie Schilling and Alexandria Marsters, 'Unmasking identity: Speaker profiling for forensic linguistic purposes', *Annual Review of Applied Linguistics*, 35 (2015), pp. 195–214.

[129]Claudia Aradau and Tobias Blanke, 'Governing others: Anomaly and the algorithmic subject of security', *European Journal of International Security*, 3:1 (2018), pp. 1–21.

[130]Carlo Ginzburg, 'Morelli, Freud and Sherlock Holmes: Clues and scientific method', *History Workshop*, 9: spring (1980), pp. 5–36.

[131]Jennie Gottschalk, *Experimental Music since 1970* (London: Bloomsbury, 2016), p. 97.

attracted by the slogans 'less is more' and 'more is more'.[132] *Proliferation (of data) and (data) excess constitute a recurrent motif in his trajectory. In his work* Dataphonics, *created for the French radio station* France Culture *in 2007, Ikeda investigates the 'sound of data' (the sound of digital data) and the 'data of sound' (the components of sound), as well as the relations between them.*[133] *Dataphonics is part of his broader art project* Datamatics *(2006–08), with which he has been exploring – in artistic forms as diverse as concerts, installations, publications, and CD releases – the potential to perceive the invisible multi-substance of data, seeking 'to materialise pure data'.*[134] *Whereas Tone's work is primarily concerned with translations between code, images, and text, Ikeda's compositions invite us to focus on the transformations of data, inside data, through data.*[135]

By introducing the tropes of composting and computing, we want to highlight data's co-constructed and situated nature. This is not a novel idea – '"raw data" is … an oxymoron' is becoming a leitmotif in much STS writ large literature.[136] Still, composting and computing show promise. For instance, they work well with composition because they are not visual tropes, contrary to many of those we use in social sciences and beyond. While they both invite an exploration of how data become something inside wider compositional frameworks, they do not force upon us compositions as visual images. Taken together, they prepare us for what Weitzel calls a 'sonic reimagining', more attuned to the study of the governance of 'flesh-and-blood bodies',[137] as well as specific and relational digital data. Indeed, data as something calls for attending to their materiality from a multisensorial perspective – resisting the temptation to limit our understanding of what data are to what we can see or visualise, or to how we have got used to picturing them. This posits the question of what kinds of compositions data make possible or facilitate. But also, indirectly, of what kinds of negotiations actors should carry out when they want to use a dataset in a different kind of composition – that is, when they compute by composting.

Contemporary composers can teach CSS something about grasping data-driven practice. They have been playing with the digital for some time already. They explore the relations between music, data, and sound, including noise, in their own way. This resonates – so to say – with Roland Barthes's attention for the contemporary evolution of music. Barthes proposes that we think about, and ultimately 'rediscover', what he defines as 'musica practica'.[138] He argues that '[t]o compose, at least by propensity, is *to give to do,* not to give to hear but to give to write.'[139] It is the ability to move 'from one source of sounds to another'.[140] Composing with sound sources then – be they music noise or anything else – is ultimately akin to the 'making something with something' suggested by Guattari.[141] In some cases, data compositions may thus become a way to question security practice, rather than perform it. And – as Ikeda's artworks teach us – computing and composting can play a role in this effort to better understand, to question and to reimagine, security compositions. Relying on music and sound art composers that sometimes happen to be computer program(mer)s too, we can reflect upon how entering into data-informed worlds might be imagined beyond *purely visual* data visions.

[132]Ryoji Ikeda, *Formula* (Tokyo: NTT Publishing, 2002), p. 7.

[133]Ryoji Ikeda, *Dataphonics* (Paris: Dis Voir, 2007).

[134]Ikeda adjusted some artworks of the 'Datamatics' project to attune them to the exhibition space at the Amsterdam Eye Filmmuseum in 2018. For more information, see {http://www.ryojiikeda.com/project/datamatics/} accessed 15 October 2018.

[135]See also on the connections between both, Adam Collis, 'Establishing a Critical Framework for the Appraisal of "Noise" in Contemporary Sound Art with Specific Reference to the Practices of Yasunao Tone, Carsten Nicolai and Ryoji Ikeda' (PhD Thesis, University of Surrey, 2016), p. 153.

[136]Geoffrey C. Bowker, *Memory Practices in the Sciences* (Cambridge, MA: MIT Press, 2005), p. 184; Lisa Gitelman (ed.), *'Raw Data' is an Oxymoron* (Cambridge, MA: MIT Press, 2013).

[137]Weitzel, 'Audializing migrant bodies', p. 3.

[138]Roland Barthes, *Image, Music, Text* (London: Fontana Press, 1977), p. 153.

[139]Ibid.

[140]Ibid., emphasis in original.

[141]Guattari in Guattari and Zahm, 'On contemporary art', p. 45.

Christina Kubisch is a German composer, musician and sound artist, active since the 1970s. She has notably developed installations that take as themes 'the worlds between hearing in the dark and seeing sound',[142] making 'hidden sounds of urban space electronically experience-able'.[143] Since 2003, she has been working on 'Electrical Walks',[144] in which audience members receive specially designed headphones allowing them to hear the sound of electromagnetic fields, mediated by magnetic induction, and are invited to walk around following pre-established routes, so they are able hear 'the hums, buzzes, and gurgles of electromagnetic fields'.[145] The headphones allow participants to experience sounds that are not detectable without or outside them, which brings these devices close to a certain idea of 'espionage technology'.[146] The sounds' immediacy, their unexpected manifestation, and their closeness 'seem to give the listener access to the secret world of things'.[147] Of course, such a secret world does not reveal the whole truth about the secret life of modern cities.[148] The use of headphones in public spaces, in any case, also fleshes out the tensions between walking in public and private listening, between public spaces and intimate sensing.[149] With these walks, invisible structures are 'musically composed', arising out of 'cash machines, security barriers, neon advertisements, antennas, WLAN, and electrical cables'.[150] Actually, Kubisch notes that security devices are 'some of the best ones' in terms of generating sound.[151] As she explains, '[w]hen you walk through [security or anti-theft systems], you get pulsating sounds that have different rhythms': from 'simple' to 'sophisticated', from too 'strong' to altogether silent.[152] In 2005, Kubisch composed *Security*, which combines recordings from security gates of fashion shops in a number of different cities.[153] This data composition is also obtained by making inaudible electromagnetic fields audible, and is concerned with the hidden dullness of such hidden reality.

According to Theodor Adorno, the very idea of composing with computers is a 'cheap joke', inevitably resulting in compositions by subjecting subjects to a series of laws alien to them.[154] Yet, Ikeda's attempts to (audio-visually) compose by materialising 'pure data' through visuals and sound get us closer to making sense of data. When we experience his artworks, we sense digital data differently. Similarly, when we wear Kubisch's headphones, we enter a sonic-scape marked by the rhythm – and the silences – of different devices, including security ones. This reduces our alienation towards data. As Marcella Lista has it, 'the spectator becomes the listener and even more, the interpreter of this composition through the simple movement of their body, associated with the sensitive membrane of the eardrum'.[155] References to purity are, however, certainly puzzling, unless we can agree that 'pure data' are *purely decayed* data. Ikeda's data are compost material, made compatible with potentially infinite computability, and composability – the '"bachelor"

---

[142]Wulf Herzogenrath, 'Foreword', in Wulf Herzogenrath and Ingmar Lähnermann (eds), *Christina Kubisch Stromzeichnungen / Electrical Drawings: Arbeiten 1974–2008* (Heilderberg: Kehrer, 2009), p. 9.

[143]Ibid.

[144]Christina Kubish, 'Electrical Walks: An Introduction to Christina Kubisch's "Electrical Walks" Series of Works' (2013), available at: {https://vimeo.com/54846163} accessed 16 April 2019.

[145]Seth Kim-Cohen, *In the Blink of an Ear: Toward a Non-Cochlear Sonic Art* (London: Bloomsbury, 2013), p. 109.

[146]Christoph Metzger, 'Mapping – contexts: the electrical walks of Christina Kubisch – cartographies through sound', in Herzogenrath and Lähnermann (eds), *Christina Kubisch Stromzeichnungen / Electrical Drawings*, p. 82.

[147]Rahma Khazam, 'From relational aesthetics to the lightning field: Christina Kubisch's Electrical Walks', in *Christina Kubisch* (ed.), *Wellenfang* (Bonn: Skulpturenmuseum Glaskasten Marl, 2010), p. 49.

[148]On the limits of the heuristic power of these walks, see Kim-Cohen, *In the Blink of an Ear*, pp. 110–ff.

[149]Labelle, *Background Noise*, p. 225.

[150]Christoph Metzger, 'Mapping – contexts', p. 81.

[151]Kubisch in Christoph Cox, 'Invisible cities: an interview with Christina Kubisch', *Cabinet Magazine*, 21: spring (2006), p. 94.

[152]Ibid.

[153]Gottschalk, *Experimental Music since 1970*, pp. 68–9.

[154]Theodor W. Adorno, *Essays on Music* (Berkeley: University of California Press, 2002), p. 657.

[155]Marcella Lista, 'The labyrinth of the continuum', in Ikeda (ed.), *continuum*, p. 13.

data' mentioned in exergue.[156] These are also the data that contemporary security practice is made of, and that critical security scholarship needs to attend to.

Digital data are the debris with which governing rationales are compos(t)ed. The composting trope connects directly to an understanding of security compositions as (eco)systems where data are unstable. In the EU PNR example discussed above, personal data can even die and be born again as anonymised data, masked data, or training data for risk assessment algorithms. Similar to what happens in Ikeda's installations, data keep becoming something else, slightly different yet potentially productive data. The volume of data and their multiple dimensions make it difficult for our senses to determine where they are coming from, and to keep track of them in an intelligible way – to the extent that we might need to ponder how they could (meaningfully) keep track of us. We know, nevertheless, that this is what they are about – tracking us together, through their being together, and regardless of whether they might become data debris, or data rubbish.

Outro

In this contribution, we have combined two tropes to better understand how digital security compositions work in practice. Our suggestion is that thinking with composting and computing we can better apprehend the role that digital data come to play in the fabric of security. We have relied on compost and computing to see data as somethings, with the ultimate purpose of better grasping how data do something (else) – tuning ourselves to the missing.[157] Composting turns our attention to how security actors attempt to digest what sounds like an excess of data, to how they try to organise noise. Computing obliges us to attend to data as both embodied and embodying somethings. Sound blends in the togetherness implied in composting, computing, and composing, with its capacity to cross material obstacles, breaking through bodies and borders, to reach the other side and merge. With sound, we can experience and understand how data interconnect in ways that the visualisation of data inevitably cannot convey as eloquently. Sounds cannot be contained inside the box; they take us directly into the *continuum* of the *continuum* of data-driven security practices.

Thinking of security practice as a matter of (data) compositions promises to enrich CSS in two ways. First, we hope to broaden our field's worldview of data-driven security. So far, critical security research mostly focuses on algorithms, centres of calculations, and data analysis.[158] In other words, this scholarship offers a compelling contribution in studying the governing *through* data. Too little attention has been paid to data structuring, curation, and integration, yet these mundane activities are crucial to make data 'algorithm ready',[159] both for machine learning and less advanced computing processes. They are also critical for security actors establishing new systems, coping with big data or simply engaged in transnational cooperation – as we have shown in our brief discussion of a European project for passenger surveillance. From this perspective, the tropes of composting and computing contribute to an emerging literature studying the politics of design and of implementation of data-driven security practice. Second, studying security practice in terms of data compositions supplements the latent visualism that informs our ways to think about the digital. Instead of discussing traditional sonic security practices (for example, wiretapping) we have focused on how data can encode sound, that is, the voice of asylum seekers. Sound turned into data means that these data can then be cross-matched, assessed, and governed. These digital data embody both migrant voices and criteria of truth – the right accent, or the right

---

[156]During, 'Ikeda, or subliminal time', p. 59.

[157]'"As unlikely publics"', to quote Brandon LaBelle, *Sonic Agency: Sound and Emergent Forms of Resistance* (London: Goldsmiths Press, 2018), p. 57.

[158]See, among others, Amoore and Raley, 'Securing with algorithms'; Jeandesboz, 'European border policing'; Bigo, 'The (in)securitization practices of the three universes of EU border control'.

[159]Tarleton Gillespie, 'The relevance of algorithms', in Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (Cambridge, MA: MIT Press, 2014), p. 168.

dialect. While similar to already studied practices of bodily surveillance, for example, fingerprinting, these sonic embodiments deserve scholarly and political attention. They rely on and reify problematic assumptions about socialisation, truth, and identity. At the same time, data turned into sound do not only facilitate security actions, as in the use of a metal detector, but may also embody apparently silent and invisible digital surveillance practices, as we heard in Kubisch's sonic compositions.

Each of Ikeda's installations has its own specific voice. You wonder whether it is a single track coming back as a loop, or whether it will keep evolving, changing indefinitely. You search for patterns, rhythm, and meaning. You attempt to connect pitches and specific sounds with what is happening on the screen – the sudden appearance of a link, the display of geometrical figures, the pinpointing of a spatial coordinate, and their continuous vanishing. Your eyes and your ears, your body, your brain: all of you soon feels overwhelmed by all these data. You see and hear data everywhere, and in everything, somehow trying to convey information that keeps moving, that is inapprehensible. The world around you speaks data, with data that are never silent, that are never fully fixed. Some visitors step into an installation, and walk upon a gigantic display on the ground. They sit down and take (digital) pictures of themselves in the midst of data flows, to be shared across data platforms. They are data swimming through data streams. You play with your own shadow on the data screens, feeling in read-only mode. You can see, you can hear, you can take more pictures. But you cannot edit, nor be fully viewed, or even heard. This may be the ideal place to start thinking.

Rocco Bellanova is a Postdoctoral Researcher at the University of Amsterdam (UvA). His work sits at the intersection of politics, law, and science and technology studies. He studies how digital data become pivotal elements in the governing of societies. His research focuses on European security practices and the role of data protection therein.

Gloria González Fuster is a Research Professor at the Vrije Universiteit Brussel (VUB)'s Faculty of Law and Criminology. Co-Director of the Law, Science, Technology and Society (LSTS) Research Group, and member of the Brussels Privacy Hub (BPH), she investigates legal issues related to privacy, personal data protection, and security.