Philosophy Study, April 2018, Vol. 8, No. 4, 183-190
doi: 10.17265/2159-5313/2018.04.004

The (Impossible) Art of Balancing National Security and Privacy in a Global Context

Anne Gerdes
University of Southern Denmark

This paper highlights the work of collaborating European journalists, who in a series of articles, under the heading "Security for Sale—the Price we pay to protect Europeans", problematise the European Union Funding framework for security technology research, which unfortunately may enhance business opportunities for mass surveillance systems in non-democratic states. Based on a case, involving a research project in which I participated as an ethical adviser, the paper illustrates how a lack of global perspectives constitutes a weakness inherent in methodologies within design ethics, such as Privacy by Design and value sensitive design. Finally, drawing on the notion of professional idealism (Mitcham 2003), the paper concludes by arguing in favour of moral activism from a global outlook, which goes beyond the walled gardens of the European Union.

Keywords: security technology, privacy, globalization, human rights, value-focused design

1. Introduction

I set out to discuss ethical dilemmas we are faced with when European Union (EU) funded research projects unintendedly support the development of, and markets for, mass surveillance systems in non-democratic states. From Primo 2013 to Ultimo 2015, I was involved in the ePOOLICE (www.epoolice.eu) research project as an ethical adviser. The ePOOLICE project developed a *proof of concept* prototype and received funding from the European Union Seventh Framework Programme. The consortium behind the project consisted of researchers and companies, one of which has subsequently been bought by a Danish company owned by a person in the United Arabic Emirates (UAE). This specific case is brought up in the Danish Newspaper Information (Andersen & Gjerding March 6, 2017), as one of a series of articles in European papers under the general heading: "Security for sale the price we pay to protect Europeans." Over a two years period, a group of European journalists have investigated how the European security industry benefits from the European Union's research funding programmes within the area of security technology for fighting organised crime and terrorism (Security for Sale homepage).

The case is used to draw attention to the vulnerability of methods to promote ethics in technology design, such as value sensitive design, (Friedman & Kahn 2004), and Privacy by Design (Cavoukian 2012). While these methods may work well in local, democratic contexts, they are easily defeated in a global context. Consequently, a call for professional idealism (Mitcham 2003), or activism, can be seen as a preliminary step towards establishing a framework, which could strengthen value-focused design methods when seeking ways to

Anne Gerdes, Ph.D., Associate Professor, Department of Design and Communication, The University of Southern Denmark, Denmark; main research fields: Robot Ethics and Philosophy of Artificial Intelligence, Privacy.

scaffold ethical values and human rights in a global perspective.

In what follows, the scene is set for a presentation of the ePOOLICE project; specifically paying attention to how privacy challenges have been addressed (sec. 2). This is followed by an account of the current case covered in news articles from the Danish newspaper Information (Andersen & Gjerding March 6, 2017; Andersen February 24, 2017) (sec. 3). Here, the journalists reveal how weak enforcement of export control regulation and lack of moral standards in a given security company give rise to concern that possible violations of human rights in the UAE might be facilitated using technology, which could very well have been developed with inspiration from the European Union funded project ePOOLICE. It is important to note that the case does not reflect function creep in the narrow sense, i.e., as when a specific technological system is transplanted to a use context, which conflicts with the purpose for which the system was originally designed and consequently causes ethical problems. However, although direct knowledge or technology transfer did not take place in the current case, it may still be argued that a kind of mission creep is at stake as the knowledge opportunities coming from collaboration in the research project may have inspired later projects and business decisions.

On the backdrop of these observations, it is problematized that there exist a surprising lack of global perspectives in moral philosophy concerning ethics of technology, as well as in value oriented design methods, such as Privacy by Design (Cavoukian 2012) and value sensitive design (Friedman & Kahn 2004; Nissenbaum 2005). Even though value sensitive design addresses the importance of paying attention to other cultures' values in design, the method does not give guidelines for situations as the current case concerning how to ensure human rights in a global perspective. As such, a call for moral activism or professional scientific idealism (Mitcham 2003) is needed in the design ethics research community.

2. The EPOOLICE Project—Balancing Citizens' Right to Privacy and Security

The European Commission's funding framework emphasises high standards of ethics. Therefore, data protection and privacy issues are key priority areas, which imply that effort enters into promoting privacy safeguards, as well as in trying to anticipate possible ways in which European citizens' privacy may be infringed by security technologies for fighting organised crime and or terrorism. Hence, the recently finalised (2013-2015) ePOOLICE project represents an open source intelligence sense-making system (realised as a prototype demonstrating a proof of concept solution), which seeks to improve the capabilities of law enforcement agencies, at the strategic level, by supporting long-term crime forecasting (Gerdes 2015).

Technically speaking, the ePOOLICE system consists of an environmental scanning system and a dynamic knowledge repository. The environmental scanning takes departure in a structured framework, including a number of societal domains, which divide the environment into political, economic, social, technical, environmental, and legislative domains, coined with an acronym as PESTEL domains (Choo 1999). On this background, environmental scanning may be carried out on data streams from a variety of open public online sources. In order to manage the mining of data streams, natural language processing text mining techniques, e.g., concept extraction and semantic categorization, may be applied to handle the acquisition, identification, and filtration of relevant data sifted from environmental scanning. Next, by fusion techniques, different kinds of data streams may be homogenized and feed into an ontological knowledge base, which, by means of learning algorithms, may gradually build up a rich taxonomy of knowledge about a given domain. In this way, it becomes possible to refine and monitor heterogeneous information sources in PESTEL domains and identify unanticipated patterns. Consequently, data processing is facilitated using data analysis techniques, which

enables the extraction of descriptive and predicative meanings used for inferring hidden states which may subsequently be merged to support law enforcement analysts' in forecasting future crime trends.

As such, the environmental scanning of public online sources provides a systematic approach for exploring and mapping patterns of information at a general level without singling out unique data subjects. Consequently, within the overall framework of the ePOOLICE project, no data subject is identified or under surveillance, and no personal and intimate information, per se, is involved in the identification of relevant data and interpretation of relevant patterns of information. However, since personal (and often also sensitive) information is highly accessible online, particularly in relation to social media data streams, the inherent risk of unintentionally identifying data-subjects during the raw data scanning process is fairly high. Here, we have to bear in mind that personal data includes information, which may identify an individual indirectly using different fragments of sources (Gerdes 2015).

Especially, social media scanning may imply privacy discomfort among people. Users on social networking platforms are typically aware that data shared on social media resides in a public or semi-public sphere. Applying privacy settings may well decrease the group of people with access to your data, but still not hinder that data is spread to others. However, we cannot per default presume that people, when engaging in producing and sharing online content on social media platforms, do not have any expectations of privacy. All though users are aware that data is, to some extent, public, it is reasonable to assume that they probably do not expect their online content to be made available as raw data sets for environmental scanning. Hence, even though this particular type of environmental scanning of social media data is in alignment with data legislation, it might still give rise to ethical concerns. Based on these observations, it was decided not to include environmental scanning of social media data in the ePOOLICE project.

In a security perspective, the prototype system exemplifies a tool for strategic intelligence led activities focusing on possible future types of modus operandi and crime trends. For that reason, personal data is not relevant in the information context of ePOOLICE, since the system does not aim at identifying individuals. Moreover, a privacy-preserving design framework has guided the system development process. For instance, even though anonymization is in general challenged in the context of open source data, it may still be helpful to apply advanced anonymization techniques as a safeguard which may reduce the risk of re-identification of data-subjects, especially in cases in which personal data are not considered useful in the first place, meaning that if personal data accidentally emerge through the merging of data fragments, they are treated as "noise."

To sum up, in seeking to balance data privacy and data utility, the system design and tool development in ePOOLICE is based on a privacy-preserving system development framework supported by legal research (Callanan et al. 2009; De Marco 2014) and in compliance with European data protection legislation. Also, an external ethical advisory board has been helpful in the process. In continuation thereof, other privacy safeguards, regarding system functionalities, have been installed, such as for instance considerations to permit management of different user-levels of authorization. In that respect, logging of system access and processes ensure tracking of possible unauthorised use of data, and further support control procedures by internal data controllers, as well as by independent authorities. A risk analysis, a Privacy Impact Assessment (PIA) has been carried out in relation to the prototype outcome of the project, and recommendations have been made to ensure that, once the system is realized, member state legislation shall authorise its use and PIAs shall be carried out on a regular basis (De Marco 2014).

Nevertheless, it goes without saying that a proof of concept prototype system like ePOOLICE might inspire the development of systems for operational purposes enhanced by social media mass surveillance, which could lead to moral wrongdoing in a non-democratic context.

3. The Newspaper Information's Revelations Highlights the Need for Moral Activism and Global Perspectives in Value-Oriented Design Methods

The ePOOLICE research project represents a typical-European Union research project consisting of a consortium of researchers, end users, and companies. According to an article in the Danish newspaper Information (Information, Andersen, & Gjerding March 6, 2017), one of the participating companies, a small start-up company, D4tec, got funding as a partner in the ePOOLICE project. D4tec also gained financial support from a public financed innovation initiative (http://www.borean.dk/en/). By the end of 2015, shortly after the ePOOLICE project terminated, D4tec started collaboration with Liace, a Danish it-company owned by a person in the UAE. As an investor, Liace also obtained rights to D4tec software products for social media scanning. This gave rise to ethical concerns among employees and caused one of the system developers to leave the company, in which he had only worked for a few months. During his job interview, he had expressed ethical concerns related to human rights in a global perspective, but, back then the management had assured him that these concerns were groundless since the company only focused on law enforcement agencies at the European security market.

However, in 2016, D4tec realised that it did not manage to "crack the market code" at the European security market, and in April 2016, the company was fully taken over by Liace. The article concludes that: "public state investment ended with a million classes loses. Moreover, the Aarhusian company, with UAE roots, now had full rights over the surveillance software" (Information, Andersen, & Gjerding March 6, 2017). Next, the journalists report that they had a hard time getting information from the company concerning what they actually do in the market. However, there are clear indications that Liace is related to Teletronics, an IT-company, which has close relations with the regime. Once again, it has been almost impossible for the journalists to figure out what Teletronics is dealing with:

> However, according to a slideshow from a presentation, which two employees gave at a conference in 2016, Teletronics is "a software company, which collaborates with Dubai to reach the government's goals about a smarter and more connected Dubai." If D4tec's surveillance technology has landed in the hands of Teletronics, which presumably is the case, it has landed in the hands of somebody, founded by and collaborating with the regime. (Information, Anders, & Gjerding March 6, 2017 [author's translation from Danish])

Moreover, prior articles in the series (Andersen February 24, 2017; Andersen et al. February 23, 2017), highlight how weak enforcement of export control rules facilitated export of technology, which could endanger human rights once applied in a non-democratic context. In 2014, the European Union decided to include surveillance technology under *the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. Hence, it is mandatory that companies shall apply for export permissions in cases involving export of surveillance technology has to be exported to countries outside Europe. However, on an European level, the journalists' investigations have revealed that these permissions are disturbingly easily granted to companies:

> During the past two years, European Member States have allowed export of surveillance technology to countries outside of the Union 317 times. These systems are, to a great extent, sold to dictator states. Approximately 30 percent of the

> permissions apply... to countries, which the think tank Freedom House's yearly report "Freedom in the World" characterises as "not free." And 52 percent of permissions go to countries, which Freedom House characterizes as "partly free." Only 17 percent apply to countries, which are "free," for instance, a country like the USA." (Information, Andersen et al. February 23, 2017 [author's translation from Danish])

It is important to underscore the fact that due to restrictions, concerning knowledge and technology transfer from the European Union funded research projects, no direct transfer from the ePOOLICE project is allowed to take place. However, it may still be argued that a kind of mission creep might be possible as the knowledge opportunities coming from collaboration in a research project may have inspired later projects and business decisions. It is also plausible that violations of human rights might be facilitated using the kind of surveillance technology developed by companies like Liace/Tectronics, with product portfolios that, to a certain extent, might rely on inspiration and ideas from research projects like the ePOOLICE project.

Continuously, there is reason to be concerned, which is also underscored by the report *Human Right Watch—United Arab Emirates Events in 2016* (HRW Report, 2017), which brings forward a series of violations of human rights. Consequently freedom of expression has been violated on several occasions, and the report states that "The UAE deployed expensive surveillance software to target leading human rights activists" (HRW Report, 2017). Likewise, in the report, of the UN Special Rapporteur Frank La Rue on the promotion and protection of the right to freedom of opinion and expression (La Rue 2014), the responsibilities of the private sector are problematised as state regulations lag behind the development of surveillance technologies. Hence, it is recommended that: "States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations" (La Rue 2014, 22).

Likewise, ethical issues related to security technologies are addressed in an opinion report by the European Group on Ethics in Science and technologies (Dratwa 2014). Here, it is suggested to deal with the global lack of legal standards related to mass surveillance technology by making bilateral agreements "with as many countries as possible. It would be obvious to start with other EU countries, and of course, the US is also a natural partner for consensus building with the EU" (Dratwa 2014, 58). Obviously, the strategy's lack of global vison is striking as it can be doubted whether the best scene for an outlook on human rights, in the era of global communication surveillance, is the walled gardens of EU and Free states.

Likewise, a lack of critical global perspectives is reflected in the work of technology theorists occupied with value oriented design methods, such as for instance, value sensitive design (Friedman & Kahn 2004) and Privacy by Design (Cavoukian 2012). Hence, privacy protection, in Privacy by Design, is promoted as a "win-win positive-sum approach" (Cavoukian 2011), encouraging companies to respond to privacy challenges from the assumption that privacy protection is not only a burden but can be viewed as a business driver. This approach is also highlighted by Van den Hoven, who argues that value sensitive design can be seen, not only as a constraint but as a source of innovation. In fact, sometimes conflicting value orientation may actually drive innovation rather than hinder it (van den Hoven 2013, 77).

The value-focused perspective in value sensitive design emphasises philosophical clarification of important values in tandem with empirical testing and user driven design methods. Within the field of value sensitive design, the global perspective typically concerns the importance of paying attention to cultural diversity (Friedman & Kahn 2004; Alsheikht 2011), as for instance in emphasising that one should not use a dog icon on a printer interface if one is targeting Islamic countries (Friedman & Kahn 2004, 1183). In

continuation thereof, designers are advised to incorporate universal values while, at the same time, respect cultural values:

> Theorists who strive to uncover moral universals believe they are wrestling with the essence of morality, with its deepest and most meaningful attributes. In contrast, theorists who strive for characterizing moral variation argue that by the time you have a common moral feature that cuts across cultures; you have so disembodied the idea into an abstract form that it loses virtually all meaning and utility... In our view, both questions have merit, and a middle ground provides a more sensible and powerful approach for the HCI community: One that allows for analyses of universal moral values, as well as allowing for these values to play out differently in particular culture at a particular point in time. (Friedman & Kahn 2004, 1182-3)

These methods should be praised for pro-actively setting out to embed ethical values in technology design on an informed groundwork, encapsulated in Van den Hoven's call for practising "front-loaden ethics" (Van den Hoven 2007). Nevertheless, typically such methods are applied with the purpose of bringing technology design in alignment with legislation and the value expectations of citizens in free countries. Alternatively, as in the case of Alshkeithk (2011), to illustrate design issues related to cultural diversity—e.g., how cultural values of intimacy unfold in an Arabic context, requiring that the designer has to seek to understand of key differences between Western and Arabic cultural norms and roles.

Hence, value sensitive design centers on clarification of conceptual and empirical analyses of human and ethical values, and how such values can be inscribed in design via stakeholder analysis. Accordingly, issues related to globalisation are mainly raised when dealing with how to reflect cultural values in design.

On the other side, *The ACM Code of Ethics and Professional Conduct* includes a global perspective in its first principle:

> This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures... When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare. (ACM Code of Ethics and Professional Conduct homepage)

The techno-scientific power demonstrated in surveillance technology is more subtle and not as immediately dangerous as the powers of nuclear weapons, which, after The Second World War, caused Niels Bohr to insist on international cooperation on nuclear energy, in an open letter to the United Nations. By the same token, and as a source of great inspiration and insights, Mitcham's account of the tradition termed *professional scientific idealism* is worth mentioning (Mitcham 2003).

Here, Mitcham highlights central historical movements, such as for instance the Pugwash movement, which arose in the aftermath of the atomic bomb, a period during which scientists increasingly saw an urgent need to respond to the dangers of the nuclear age, and, as an example thereof, "it was a Pugwash proposal... that made possible the 1963 Limited Nuclear Test Ban Treaty" (Mitcham 2003, 255). Likewise, the Union of Concerned Scientists (UCS) was founded in opposition to the Vietnam War. Consequently, at MIT, faculty staff issued a declaration based on the awareness that technology needed to be controlled, and that scientists and engineers ought to take an active part in the shaping of public policy issues concerning the societal impact of technology. Today, organizations like UCS, The Federation of American Scientists, and The Committee on Scientific Freedom and Responsibility, under the American Association for the Advancement of Science, represent influential voices in "the social reconstruction of technology" (Mitcham 2003, 256). Over the years, the agenda of moral criticism has been expanded to also include topics such as professional codes of ethics and human rights.

These movements and organizations have attempted to promote human flourishing, using techno-scientific moral criticism. Due to the inherent complexities of human-technology interactions, this has not always been accompanied by "simple or unequivocal success" (Mitcham 2003, 256). As such, Mitcham notes that all though we are not determined by technology in the strong sense, we are nevertheless challenged by the way technology and science shape us, and the way society shape technology: "Given the exigencies of techno-economics, not to mention those of human nature, there seem to be tendencies or trajectories of use embodied, if not in the techno-science alone, then certainly in the techno-science-society interface, that is often extremely difficult to sidestep" (Mitcham 2003, 257).

This observation reminds us of the importance of having a realistic sight on the complexity of the challenge we are facing when we commit ourselves to techno-moral activism. However, it does not imply a "technological-progress-as-directed-tragedy"-viewpoint (Lowrance 2010, 44), which leaves us without the choice of changing things for the better once the technology has been developed and transferred to usage contexts that give rise to moral concerns.

Obviously, the above-mentioned observations demand that I scrutinise my role as an ethical adviser eager to promote a privacy preserving design agenda. I need to ask myself, whether I ought to have anticipated that this project might end up having funded and, presumably, inspired a company without moral standards? I think it is reasonable to say that I ought to have foreseen that although technology and direct knowledge transfer was not at stake, a global critical perspective should have been invoked, and in that case, this would have enabled me to foresee the current scenario. My motivation for participating in this project was steered by the fact that the project was aimed at strategic purposes and not intended for surveillance of individuals. My basic assumption was that we could do engineering activism, a term coined by Nissenbaum (2001), which echoes the quest for a pro-active stance towards the challenge of bringing ethics to design, but, as mentioned above, without highlighting global issues. In the case of ePOOLICE, this was realised by promoting a privacy preserving design framework, which brought technology into alignment with European legislation and stakeholders' value orientations in the context of how the balance of security and privacy is valued in the European context. This perspective overshadowed my concerns about global perspectives and use scenarios, such as whether the ePOOLICE project might generate a financial or inspirational spinoff with unethical consequences in non-democratic countries.

I ought to have considered, but never did worry, whether current export control legislation was being enforced as expected or not, especially since the above-mentioned revelations suggest that all over Europe it seems to be easy to get an export permission allowing for surveillance technology export to non-democratic states. This lesson widens the scope of the domain we need to encompass when seeking to anticipate ethical challenges using value-focused design methods.

4. Concluding Remarks

The lesson, learned from my participation as an ethical expert in the ePOOLICE project, is that there is no free lunch: The bill for balancing privacy and security on the backdrop of a democratic foundation could end up being paid by those, who lack human rights. Hence, I might consider giving up participating as an ethical adviser on future European research projects, since in this position, I could risk ending up serving as a shallow moral blueprint. On the other hand, I might stay and attempt to do moral activism by highlighting a call for action within the research community as well as at the policy level, and certainly also within the field of design

ethics. Here, there is a need to start working on a revised research agenda, which emphasise global responsibilities.

Works Cited

ACM Code of Ethics and Professional Conduct. March 6, 2017. <https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct#imp1.3>.

Alsheikht, T., Rode, J. A., and Lindley, S. E. “Whose Value-Sensitive Design? A Study of Long-Distance Relationships in an Arabic Cultural Context.” CSCW 2011, 2011.

Andersen, L. S. and Gjerding, S. “Dansk Overvågnings software udviklet for skattekroner opkøbt af firma i diktaturstat.” March 6, 2017. Information, 2017.

Andersen, L. S. “En digital lejesoldat deserterer.” February 24, 2017. Information, 2017.

Andersen, L. S., Gjerding, S., and Goslinga, M. “Europa eksporterer spionteknologi til diktaturstater i stor stil.” February 23, 2017. Information, 2017.

Callanan, C., Gercke, M., De Marco, E., and Dries-Ziekenheiner, H. “Internet Blocking—Balancing Cybercrime RESPONSES in Democratic Societies.” March 6, 2017. <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>.

Cavoukian, A. “Privacy by Design the Seven Foundational Principles.” March 6, 2017. <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

---. “Privacy by Design from Rhetoric to Reality.” March 6, 2017. <https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>.

Choo, C. W. “The Art of Scanning the Environment.” *Bulletin of the American Society for Information Science* 2-3 (1999): 21-24.

De Marco, E. EPOOLICE. “Deliverables D3.3. WP3—Technical and Legal/Ethical Constraints and System Framework Design.” March 6, 2017. <https://www.epoolice.eu/EPOOLICE/servlet/document.listPublic>.

Dratwa, J. “Ethics of Security and Surveillance Technologies.” Brussels, 20 May 2014. March 6, 2017. <http://ec.europa.eu/DocsRoom/documents/11493>.

Gerdes, A. “EPOOLICE Security Technology—Fighting Organized Crime Whilst Balancing Privacy and National Security.” *The 10th International Conference on Cyber Warfare and Security, Krüger National Park, South Africa*. Ebook ISBN: 978-1-910309-97-1, 2015.

HRW. “Human Right Watch—United Arab Emirates Events in 2016.” March 6, 2017. <https://www.hrw.org/world-report/2017/country-chapters/united-arab-emirates#eaa21f>.

La Rue, F. “Report of the Special Rappoteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” March 6, 2017. <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>.

Lowrance, W. “The Relation of Science and Technology to Human Values.” Ed. C. Hanks. *Technology and Values—Essential Readings.* Sussex: Wiley-Blackwell, 2010. 38-49.

Mitcham, C. “Professional Idealism among Scientists and Engineers: A Neglected Tradition in STS Studies.” *Technology in Society* 25 (2003): 249-62.

Nissenbaum, H. “How Computer Systems Embody Values.” *Computer—Innovative Technology for Professions* 3 (2001): 117-9.

---. “Values in Technical Design.” Ed. C. Mitcham. *Encyclopedia of Science Technology and Ethics*. New York: MacMillam, 2005. 66-70.

Security for Sale Homepage. March 6, 2017. <https://thecorrespondent.com/10221/security-for-sale-the-price-we-pay-to-protect-europeans/497732037-a3c8cc9e>.

Van den Hoven, J. “ICT and Value Sensitive Design.” Eds. P. Goujon, Lavelle, S., Duquenoy, P., Kimppa, K., and Laurent, V. *IFIP International Federation for Information Processing Vol. 233, The Information Society: Innovations, Legitimacy, Ethics and Democracy.* Springer: Boston, 2007. 67-72.

---. “Value Sensitive Design and Responsible Innovation.” Eds. R. Owen, J. Bessant, and M. Heintz. *Responsible Innovation.* Wiley & Sons, Ltd. Published, 2013. 75-83.