Summary for *ACM SigComm2015 – Ethics in Networked Systems Research*

RoboCode ethicists – Privacy-friendly robots, an ethical responsibility of engineers?[1]

Christoph Lutz
Institute for Media and Communications Management
University of St. Gallen, Switzerland, PhD Student
christoph.lutz@unisg.ch

Oxford Internet Institute (Visiting PhD student 2015)
University of Oxford, United Kingdom
christoph.lutz@oii.ox.ac.uk

Aurelia Tamò
Chair for Information and Communication Law
University of Zurich, Switzerland, PhD Student
aurelia.tamo@uzh.ch

Institute for Pervasive Computing (Visiting PhD student 2014/2015)
ETH, Zurich
aurelia.tamo@inf.ethz.ch

[1] A full version of this article has been submitted to the ACM Web Science conference and is currently under review.

Summary:

The robot revolution is well on its way. A current estimation assumes that between 2013 and 2016, 22 million robots will be sold (IRF World Robotics Report, 2013). Robots – defined as a "machine situated in the world that senses, thinks, and acts" (Bekey, 2012, p. 18) – are currently used in many professional and social contexts, such as labor and services, military and security, research and education, healthcare, as personal companions or toys. Severe social implications arise with the increased diffusion of robots. These implications cover topics as broad as security, displacement of human labor, anthropomorphism, cyborg visions – and privacy threats.

However, technological advancements have led to controversies and fears around privacy long before the robot revolution (Smith, Dinev, & Xu, 2011). Automated data processing machines have had a disruptive impact on the way information is collected, analyzed, employed or shared. The rupture embodied by seamless, dehumanized and sometimes invasive collection structures as well as intransparent processing patterns has raised privacy concerns – not only in social science but also in computer science (Langheinrich, 2005). The described abilities of robots to sense, think and act upon the world around them likewise stir up privacy concerns. However, while there is a rich body of literature on robot ethics (Gips, 2011 for an overview), research on robots and privacy is only in its infancy. Robotic privacy can be analyzed within the wider margin of robot ethics, which deals with up-rising question such as "what should robots do?" and "what laws and rules should robots obey to?".

Our focus lies on autonomous and social robots and the privacy concerns they raise. Such robots might present privacy threats, such as increased surveillance and access to personal information or feelings, in particular through the social bonding exhibited between humans and (anthropomorphized) robots (Calo, 2012). Two additional issues that are already described in other contexts (e.g., Internet of things, big datacome up too, namely, the opacity

of robotic technology, i.e., the fact that robots will become a taken for granted part of our everyday lives and "melt" into our environments; and the black-box-problem. The latter describes our unawareness of what robots do and how they function – especially how the algorithms work that they apply.

The literature in robot, machine, computer, and information ethics – a field with a long tradition –presents a useful set of concepts to productively approach the privacy implications of robots. In this context, two clashing rationalities that vastly correspond with two dominant perspectives in ethics in general and robot ethics in particular can be contrasted: the *developer's rationality*, which largely follows a consequentialist – means-end-rational – approach ("Make it work"); and the *regulator's rationality*, which largely follows a deontologist – value-based – principle ("Respect privacy").

The ensuing tension between these perspectives calls for alignment. The question arises whether developers should be submitted by regulation to consider privacy implications beforehand? Should privacy-friendly RoboCode be the default? The literature on how much robot engineers should encode ethical and legal standards when building their devices is divided – also in terms of privacy. On the one hand, proponents of a more constructivist approach to technology argue more in favor of a Laissez-Faire approach (Doctorow, 2014). On the other hand, Calo (2014) argues in favor of new regulation with respect to the robotic industry. We posit that it there is a middle ground, where engineers and regulators come together and their rationalities are reconciled. This can be done by taking a bottom-up aor a top-down approach. The bottom-up approach takes robot engineers as the starting point and presents them with clear-cut, feasible principles to implement privacy during the development stage (Lederer, Hong, Kay, & Landay, 2004). The top-down perspective starts from the regulator's perspective. However, instead of offering abstract notions, it operationalizes

privacy protection with a set of implementable rules. Privacy by design is a good example for the top-down approach (Cavoukian, 2009).

Both the bottom-up and top-down approach call for an alignment and a holistic view on the topic. Simultaneously there is a need for specialization in terms of the training/education of robot scholars. Philosophers, ethicists, legal scholars and social scientists working on the topic should be adequately trained in the technological aspects (especially programming and code), while engineers should possess a basic understanding of the privacy implications and theories currently discussed in the study of information systems in general and robots in particular. Robotics is a complex, interdisciplinary research field. It calls for greater specialization and experts among others in the areas of computer science, mechanics, and psychology. Like the need for algorithmists for big data analysis (a term coined by Mayer-Schönberger and Cukier, 2013), who act as "reviewers of big-data analysis and predictions" (Mayer-Schönberger and Cukier, 2013, p. 180), robotics needs "*RoboCode-Ethicists*". Such independent individuals or entities could monitor developers work, evaluate the data processing practices of robots, the choice of analytical tools, the bounding between robots and humans, the pervasiveness of data collection, and determine whether privacy implications have been deliberated about before the development of a prototype (Veruggio, 2007).

References

Bekey, G. (2012). Current Trends in Robotics: Technology and Ethics. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 17–34). Cambridge, MA: MIT Press.

Calo, R. (2012). Robots and Privacy. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 187–202). Cambridge, MA: MIT Press.

Calo, R. 2014. Robotics and the New Cyberlaw. *SSRN Electronic Journal*, 101–146. Online: http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Calo-Robotics-and-the-New-Cyberlaw.pdf

Cavoukian, A. (2009). *Privacy by Design – The 7 Foundational Principles. Information and Privacy Commissioner of Ontario*. Online: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Doctorow, C. 2014. *Why it is not possible to regulate robots here*. The Guardian Technology Blog, Robots, April 2 2014. http://www.theguardian.com/technology/blog/2014/apr/02/why-it-is-not-possible-to-regulate-robots

Gips, J. (2011). Towards the Ethical Robot. In M. Anderson & S. L. Anderson (Eds.), *Machine Ethics* (1st ed., pp. 244–253). Cambridge, UK: Cambridge University Press.

IRF – International Federation of Robotics (2013). World Robotics Report 2013. Summary online: http://www.designnews.com/author.asp?doc_id=272797

Langheinrich, M. (2005). *Personal Privacy in Ubiquitous Computing: Tools and System Support*. Dissertation submitted to the Swiss Federal Institute of Technology Zurich. Online: http://e-collection.library.ethz.ch/eserv/eth:28011/eth-28011-01.pdf

Lederer S., Hong, J. I., Key, A. D., & Landay, J. A. (2004). Personal Privacy through Understanding and Action: Five Pitfalls for Designers. *Journal of Personal and Ubiquitious Computing, 8*(6), 440–454.

Mayer-Schönberger, V. and Cukier, K. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think.* HMH Books, Boston (MA) & New York (NY).

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.

Veruggio, G. 2007. *EURON Robotics Roadmap*. Online: http://www.roboethics.org/index_file/Roboethics%20Roadmap%20Rel.1.2.pdf