Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective

Last Modified on 29/01/2019 10:50 am CET

Author: Lilian Edwards

Date of publish: January 2016

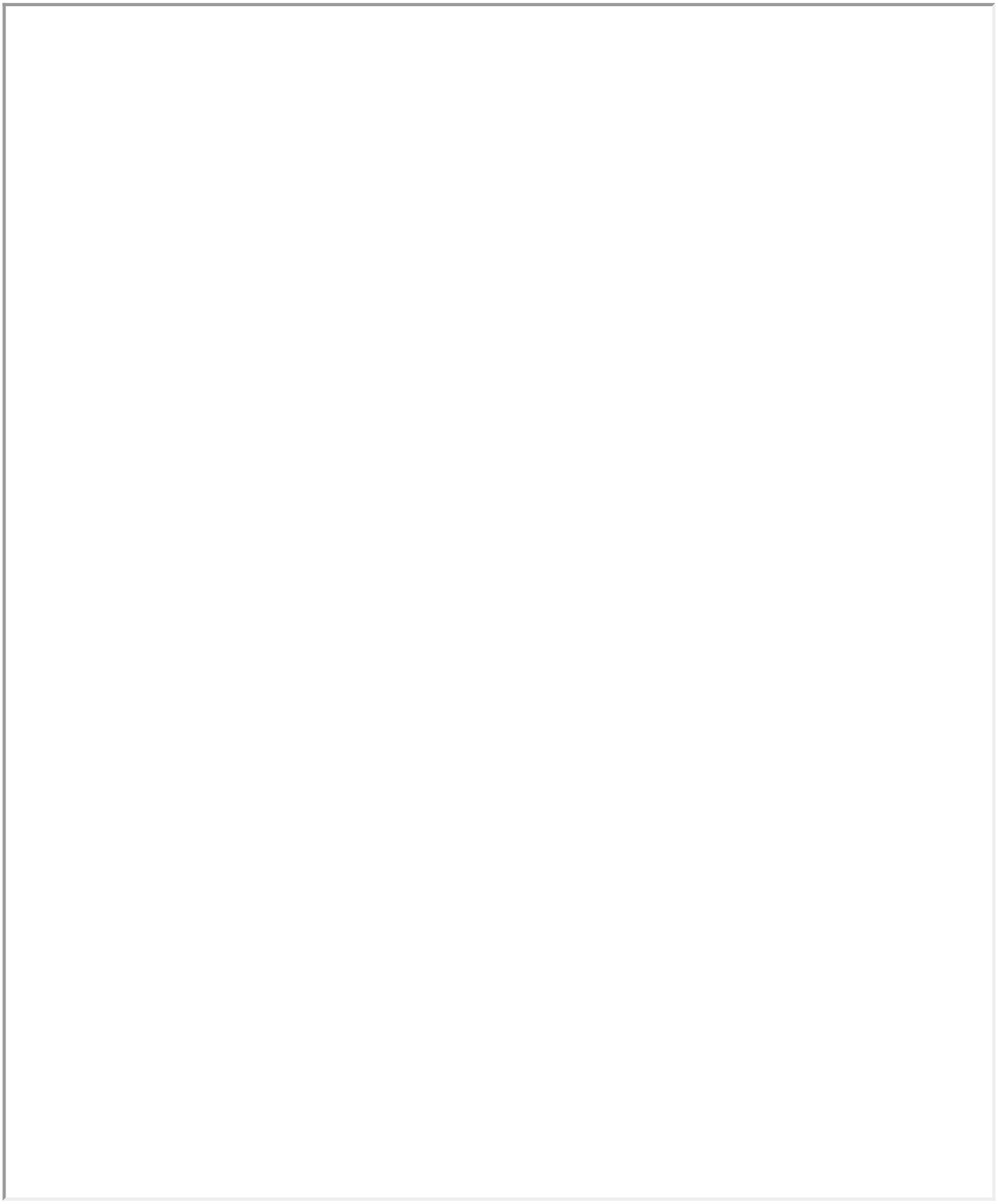
Why did we conduct this research:

The great potential of smart cities seems to be clear: more sustainable, citizen-focused areas where people are increasingly able to thrive. Nevertheless, the potential threat posed by the power of those holding the large amounts of data of these citizens cannot be neglected. Edwards explores those less attractive aspects of smart cities.

Key findings:

- Smart cities integrate the three greatest current threats to personal privacy: the Internet of Things(IoT); "Big Data" ; and the Cloud (and for which there is still no effective regulation).
- The dependence on technological infrastructures, big data, the IoT and the Cloud; together with the financing and therefore “ownership” (normally by public-private partnerships) of smart cities pose a great threat to citizen's privacy.
- The author proposes four further points in which both research and legislative involvement is needed in order to successfully build safe smart cities (from the privacy perspective), being these the investigation of: the potential for a smart city PIA or DPIA; the technical and social potential of methods of giving “pre-consent” or “sticky consent” to deal with the constraints of the IoT; legislation for algorithmic transparency and researching ways of making algorithmic data comprehensible to consumers; and moving (at least partially) away from consent or “notice and choice” as a

main mechanism for validating data collection and processing.



Reference:

Edwards, Lilian, Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective (January 5, 2016). European Data Protection Law Review (Lexxion),

2016, Forthcoming.