Crime Applications and Social Machines: Crowdsourcing Sensitive Data

Maire Byrne Evans, Kieron O'Hara, Thanassis Tiropanis, Craig Webber
University of Southampton
Southampton, U.K.
{me1g11,kmo,tt2}@ecs.soton.ac.uk, c.webber@soton.ac.uk

ABSTRACT
The authors explore some issues with the United Kingdom (U.K.) crime reporting and recording systems which currently produce Open Crime Data. The availability of Open Crime Data seems to create a potential data ecosystem which would encourage crowdsourcing, or the creation of social machines, in order to counter some of these issues. While such solutions are enticing, we suggest that in fact the theoretical solution brings to light fairly compelling problems, which highlight some limitations of crowdsourcing as a means of addressing Berners-Lee's "social constraint." The authors present a thought experiment – a *Gendankenexperiment* - in order to explore the implications, both good and bad, of a social machine in such a sensitive space and suggest a Web Science perspective to pick apart the ramifications of this thought experiment as a theoretical approach to the characterisation of social machines.

Categories and Subject Descriptors
H.1.2 [User/Machine Systems] *Human information processing.*
K.4.1. [Computers and Society] *Public Policy Issues*

Keywords
Open data; crime data; transparency; trust; social machines. network science

1. INTRODUCTION
In "Weaving The Web", Professor Sir Tim Berners-Lee explains that, "Real life is and must be full of all kinds of social constraint – the very processes from which "society" arises. Computers help if we use them to create abstract social machines on the Web: processes in which the people do the creative work and the machine does the administration." [3]

Is there any combination of person and computational system that isn't a social machine under this description? If almost any combination of human and computing device can be a social machine, how can we start to understand how these work, without being more specific?

How can we make predictions about success factors under such a general description? Does a social machine have to incorporate a "machine" in the sense that we might think of a computer, or can machine be used in the wider sense, as in some sense of a Turing Machine; a series of computations? And how can social machines actually cope with the "social constraint" Berners-Lee referred to – the "processes from which 'society' arises"? Is it possible, for example, to use crowdsourcing, or combinations of social networks, the web and mobile phones to "fight crime", as Luis Von Ahn[1] has suggested? In order to explore some of these questions, we look at them within the context of Open Crime Data in the U.K.

The structure of this paper is that first, we consider U.K. open crime data *(*data that can be freely used, reused and redistributed by anyone) and discuss social, technical and policy issues arising from its collection. Second, we discuss an app in development that might exemplify a solution – a social machine - to these current problems with crime data. We consider what questions this raises, from the perspective of a thought experiment or *Gedankenexperiment*. We finally consider these questions, both with regard to the real problems caused by such an app, and also how these real world problems might inform the classification and definition of social machines.

Lack of space prevents robust criminological discussion, and a deep exploration of existing social machines, although such considerations will be made in more depth in other work.

2. CRIME DATA
Currently the U.K. government uses crime open data via the website *www.police.uk* in order to help further the transparency and accountability programme for the policing and criminal justice system. *Www.police.uk* is pivotal in the Government's policing and justice reform agenda; through helping the public to hold their local police to account, with this accountability mediated by Police and Crime Commissioners (P.C.C.s). Crime data coming from 43 U.K. police forces is represented visually on street-level maps; inputting a postcode, name of a town, village or street takes the visitor to the crime map, or they can examine the open data that feeds the maps.

2.1 Measuring Crime
Although the website has had over 200,000 hits a day since it first came into use, (averaging over 340,000 in January 2013), showing huge public engagement with this information, there are problems with this recorded crime data, particularly where it relates to attempts "to measure the amount, nature and distribution of crime in society."[19] From deciding a crime has occurred, to reporting and recording, there are areas in which the data can mislead.

WWW 2013 Companion, May 13–17, 2013, Rio de Janeiro, Brazil.
ACM 978-1-4503-2038-2/13/05.

[1] "…social networks and cell phones really helped the revolutions in the Arab world…in the same way, it is possible for them to help address things like crime in Latin America." http://www.ipsnews.net/2011/07/qa-captcha-creator-would-like-to-tap-crowdsourcing-to-fight-crime/

Although the figures appear to be changing [17] certain types of crime are still reported to the police more than others as a result of, for example, economic and insurance incentives. Police may feel that dominant problems in a neighbourhood are car crime and burglary, while sexual assault, domestic violence and similar crimes remain under-reported. [10] "Victims of domestic violence or rape may worry about whether the police will take them seriously or whether they will face reprisals." [18] Recently recognised in the U.K. as a crime, stalking can be hard to quantify. When does knowledge of a loved one's movements become privacy-threatening surveillance? Confronting domestic abuse can depend on the victim realising that a crime has taken place, that abuse is predicated by their mental state, not just the commission of aggressive acts at specific times. There may be negative consequences for victims if they report these crimes, not only from attackers, but psychologically, morally and socially. It is hard to quantify and act on these sorts of crime, given normal police reporting mechanisms which are geared around the notion of crime as a digital event, both as the victim perceives it, and as it is enacted, not an analogue process.

Each of the 43 police forces has its own reporting procedures and practices. The Information Commissioner's Office (I.C.O.) is risk-averse with regard to privacy and the current data protection paradigm, so police data is anonymised and aggregated with little victim consultation since geolocation is privacy-threatening[2]. Data often only arrives at *Police.uk* after a period of 4-7 weeks. The data indicates trends, but is not up-to-date or accurate enough to be able to help in tracking crimes as they occur - descriptive but not predictive of crime. Other forms of data gathering occur through victim surveys, such as the British Crime Survey, (B.C.S.) suggesting a "dark figure" of unrecorded crime. For example, in contrast to open police crime data, victim surveys show that only 15% of victims report to the police and that of reported crimes, conviction rates are around 30%. Five per cent of females have been victims of a serious sexual offence since they were 16, 20% have been a victim of some sexual offence since they were 16 and 2.5% of females and 0.4% of males had been victims of sexual offences in the previous 12 months. [13]

It is recognised that "official" U.K. crime data is problematic, and that the trust of communities in the police needs rebuilding, so that "information about crime flows from the community to the police. Information is the lifeblood of solving crime." If police work is knowledge work, rather than the public sphere conception of crime fighting, it seems that current systems do not have enough of a sociotechnical approach to the production of knowledge coming from victims. Instead this knowledge is shaped by reporting systems and institutional demands for knowledge.[3] [7] This causes skew - victim survey data is geared around perceptions of "fear of crime" predicated on events that victims have experienced. These events should theoretically correspond to the U.K. Police Open Data, if the crime has been reported and recorded. However, there is no overt correspondence, yet crime policy is very much driven by reference to this "fear of crime". This places data in difficulty; neither data set solves the problems that it could, while policy hangs off data about public perception of crime that does not align with recorded crime figures.

2.2 Theoretical Solutions

With the technology now available, can we address these problems? Researchers from The Korean Advanced Institute of Science and Technology (KAIST) have an app in development – *Risk Alert* - that allows the crowdsourcing of reports on crime and that allows gradual and victim-led levels of disclosure, as opposed to the (mostly) one-size-fits-all I.C.O. data protection paradigm.

Risk Alert uses open data sources, such as crime open data, to supplement environmental information provided by users: showing floating population, hospitals, police stations, CCTV. *Risk Alert* shows a mapped location-based environmental risk score, and enables reporting of violence, harassment or threatening behaviour either to police, friends or family. Users assess their own environment to give risk scores and comments on their current location, checking for nearby police stations, broken streetlights, or suspicious behavior and can report assaults.

3. THE THOUGHT EXPERIMENT

Risk Alert sits within a coterie of apps that address the issue of violence. "These deployments…guide the women facing violence to resources and help. Most of all, these initiatives create testimonies and offer the victims a presence and a voice…crucial in the aftermath of crimes where victims are coerced into silence or purposefully isolated."[6][5][2]. However our *Gedankenexperiment* takes a deliberative step back from such apps, in that we consider how the "declarative social machinery" that they represent enables us to ask questions about privacy, trust and accountability and other forms of "social constraint", from the outset and about whether we currently have nuanced enough concepts to understand the impact that such a social machine might have.

Without actually deploying this system, we can imagine that it could very easily be used to crowdsource data, while allowing victims control over the process of disclosure – this system is analogue, rather than the digital "either-it-is-a-crime-or-it-isn't" of the formalised reporting system that feeds U.K. open crime data. It takes a step forward from "tiplines" such as http://www.crimestoppers-uk.org in the UK, as information is not mediated by the authorities before being represented. Whereas a telephone hotline that allows reporting of crimes anonymously could still be said to be a sort of social machine, such systems have information filtered in a way that allows for crowdsourcing but does not then represent information in a distributed fashion.

Our hypothetical app is similar to *http://www.patientslikeme.com/* in allowing users to decide how much they disclose. It might have predictive properties, since crime data should end up being more locatable, informative and up to date, and therefore be used to help prevent crime. Such a system expands on the currently available older, verified, government open data, not necessarily contradicting it, creating a "grey figure" from more up-to-date, less verified and less formalised data. It would enable the building of trust in the reporting system; trust is a key concept with reporting some crimes. It is recognised that technical architectures can shape realities; this could be one of the new architectures that help re-shape knowledge and experience of crime. [12] This system could create contextualised, narrative-based, community

[2] See http://www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/crime_mapping_advice.ashx for fuller explanation.

[3] "The 'forms police' work hard to restrict the narrative capacity of police officers. This restriction has evolved through successive changes to the communications formats of reports... from an open narrative to fixed-choice risk classifications."[7]

knowledge about crime with an understanding of how current recording systems shape our knowledge of crime. And of course, such a social machine changes the dynamic of the current transparency regime where performance data are produced by those very people who are being held to account - with the resulting sometimes tragic consequences. [4] This now allows for the crowdsourcing of data on crime which then can be matched against the statistics produced by the police themselves, and dialogue about accountability is fed by richer, multi-dimensional data.

We must however ask how differently might such a machine be used, for example, in Europe and Asia? We come up against notions of identity and privacy as mediated - or not - by anonymisation predicated on the U.K.'s old data protection regime; these notions are vastly different as we traverse the globe, which such an app could easily do. Globally there are legal treatments of data that would make a huge social impact if somehow incorrectly deployed. If we have certain expectations of privacy in the U.K. we trust that our data will not be exposed in a way that reveals our identity. We must consider not just "the cyber-infrastructure of high-speed supercomputers and their networked interconnections, but the even more powerful human interactions enabled by these underlying systems." [9] We must consider risk - such a reporting architecture could be dangerous, if identities were leaked, lost or let slip. We have to consider provenance – data will not be auditable without raising a lot of questions about its reliability. It would be open to trolls, to false reports, and the risk of vigilantism. Some of these issues could be addressed by the use of forensic linguistic analysis and machine learning techniques to check for unusual patterns of activity, or for one voice submitting multiple reports. However, overall, these questions make us think about how such an app stretches existing social understandings and norms when it has the capacity to bring people together globally? Could it solve more problems than it has created? Is it what Morozov calls "solutionism", an "opiate of gamification, algorithmic surveillance, and technological determinism?"[5] How do we treat issues of trust, privacy, legality and ethics? Do we need to create global systems that impose global standards or systems that are flexible enough to allow for local technically mediated interpretations of the very social constraint that drives the need for such machines? For example, *www.Ushahidi.com* is used as a global crime-reporting platform, but presumably some of the information it holds is not just lifeblood for solving crime but could potentially spill the lifeblood of those using the system. Can these questions enable us to deepen our understanding of social machines and the issues we might encounter in trying to solve these problems?

4. CRIME SOCIAL MACHINES

Having asked these questions about social and legal norms, we can go a little deeper into the characterisation of social machines in order to see if we can further illustrate some of the inherent difficulties with a machine that helps with such sensitive data.

What creates a successful social machine? What drives people to use the machine? What incentives are there? In the case of a crime-reporting system we can see that a user might be asking for help, while contributing to a sensitive crime dataset - an apparently straightforward incentive. Incentives often map into knowledge representation in these machines. How easily is this done in the case of assault or abuse data? To return to our thought experiment, and the app, we know that self-identification increase a victim's feeling of threat [1][14] along with self-blame, guilt, shame, humiliation, fear of the perpetrator, of not being believed or of being accused of playing a role in the crime and lack of trust in the criminal justice system. These fears are significantly less applicable in an online setting owing to the anonymity of the Web, which allows the victim to disclose as little or as much of what has happened as they choose, as previously discussed. It seems mediating crime reporting via web-based social machines provides a good incentive.

But when discussing incentive we must define what this is. In the case of a victim of crime, we must surely refer first to their inner knowledge of the crime, as an incentive for reporting the crime and thus their mental or cognitive state. It is this state which persuades the user that by carrying out act A, the act of contributing to the social machine, they will achieve goal B, their desired end result. A and B together create the incentive. However, to understand the mental state, or successive mental states of a victim of domestic abuse is a complex process. As stated above, one of the problems with reporting domestic abuse is recognition on the part of a victim that a crime has taken place. Research shows that this "knowledge of crime" actually ebbs and flows in the mind of the victim, if we are to talk of a mental state, goal or intention, which maps into knowledge that is to be captured and represented by the machine. How do we map these analogue and fluctuating states of knowledge of crime from a crime victim and therefore, incentives, into characterisation of social machines? We turn to further definitions of social machines in order to explore this question.

4.1 Computer mediated social interaction

Following Berners-Lee's definition above, we find another definition coming from Robertson and Giunchiglia. [15] They state that the ubiquity of personal devices and sensors changes the way we think about computation. A social computation is one for which an "executable specification exists but the successful implementation of this specification depends upon computer mediated social interaction between the human actors in its implementation". They isolate the initiation of social computation, individuals' roles in computations and the reinforcement of adopted specifications, concluding that considerations of understandings of incentive structures aligned with relevant populations let us consider knowledge representation and formal specifications in new ways. This elegantly hones our definition of social machine, but leaves the "social" element largely unaccounted for. We know that evolved machines (as with much technology) are underpinned with often perverse, unintended human interactions, that intentions can ebb and flow in users' minds, we know of the to-and-fro of a victim unsure whether or not they are a victim, creating difficulty in formalising their intentions, and that there are differing incentives on the part of those who "own" the machine and those who contribute. In fact these varying incentives can make formal specification at least onerous and perhaps even impossible if we try to isolate predictors for success.

Rather than proceeding from a top-down, definitional approach, we can try to identify and characterise social machines via bottom-up, empirical examination. We can look at common aspects of generally agreed social machines: their inputs, outputs

[4] http://gu.com/p/3e4b8

[5] http://davidsasaki.name/2013/02/future-imperfect-evgeny-morozov-vs-steven-johnson/

and computational processes, for example. The following are often agreed to be robust examples of social machines:

Table 1. Examples of agreed social machines

The DARPA balloon challenge is a competition exploring the roles the Internet and social networking play in the timely communication, wide-area team-building, and urgent mobilization required to solve broad-scope, time-critical problems.	The Obama election campaign. See for example [11] on how "seamless integration of social media and microblogging with the use of big data on clickstreams to track opinion…combined with offline door-to door operations" helped Obama win.
http://www.ushahid.com crowdsources information on conflict or violence using multiple channels such as SMS, email, Twitter and the Web.	http://duolingo.com/ enables the learning of new languages while translating texts on the web.
http://fold.it/portal/is a computer games with a purpose (GWAP) enabling citizen science contributions.	http://www.galaxyzoo.org/ Citizens classify large datasets of galaxies.
RECAPTCHA is a CAPTCHA service that helps to digitize books, newspapers and radio shows..	https://www.crimereports.co.uk/CrimeReports helps reduce, prevent and solve crime by enabling citizen dialogues with law-enforcement agencies.

The SOCIAM group[6] is analysing characteristics that these and other identified social machines have in common. [16] Some points concern organisations of person and machine and whether they are used altruistically or selfishly, and refer to "tasks", "purpose", "motivations and incentives": "the social structure and motivation that sustains continued participation in these systems".

4.2 Genetic Variation

Looking at incentives we found a difficulty in the mapping of an analogue representation of knowledge of crime in the mind of a user, seen as a sub-component of the machine. Can we define intentions and goals from another perspective, applying an evolutionary view? Do social machines have elements of non-random genetic variation, advantageous to characteristics that enhance their reproduction? Each user varies in terms of their intentions as they build into the machine – if the machine survives, then the variation in the minds of its users as they use it or build into it has led (truistically) to the machine's survival as we analyse "successful" machines. *"Selection does not have a long-term goal…selecting those characteristics that are advantageous within the environment at that...time*." [8] [4] But we find that it is this very "genetic variation" that makes looking for certain characteristics that *specify* social machines hard, depending on the ecological circumstances of their users of whose evolving and mutating intentions, goals or incentives we can not speak authoritatively. Neuroscience casts doubt on whether we can relate intention to behaviour at all; less skeptically, going back to the victims reporting crime, we have evidence that victims of domestic violence do not experience crime as a single, digital, fixed-state event. Their knowledge of their experience of the crime evolves and mutates in a way that makes such a social machine seem like a solution to the problem of reporting, but it also makes mapping intentions as a form of knowledge representation into system specifications an act of epistemological wrangling.

5. CONCLUSIONS

Whereas the goal or task element (and therefore the intention behind it) of a Turing Machine is fundamental to its definition, [20] we argue that the social machine is distinct; it is not ontologically or epistemologically viable to refer to individuals' goals on a large scale, as defining specification. The social element of these machines means that intentions may be useful in *describing* the work of these machines but may not help *define* characteristics that enable us to *predict* which machines may succeed or go "viral". We might begin an account examining the overall behaviour of the machine as something ontologically distinct from the inner states of its users, and where a goal can be specified as something that is emergent; defined, for example, via empirical observation of network characteristics of users' behaviour en-masse. Network Science aligns itself easily with large–scale phenomena, such as "genetic" variation, allowing behavioural analyses that might have predictive success. We suggest that a social machine could be defined as a Turing Machine where goals are mapped out as emergent exogenous behaviours defined via network characteristics. Key elements are: network characteristics, efficiency, omnivorous and sometimes large-scale and / or aggregated use of data, and aligning incentives correctly between the social and the machine.

So is it possible to balance a meaningful discussion of incentive against the behavioural Network Science approach advocated above? Can we run small-scale, empirical, crowd-sourced crime-reporting experiments to explore some of the issues around using Network Science in order to make predictions about the success of such a social machine while using interviews and discourse-based methods to understand more the feelings, intentions and "goals" of victims? Or should we confine ourselves to thought experiments? Can we really define a system that creates knowledge of crime to offset current open crime data or victim survey data? Could such a system change the transparency agenda – showing that crowdsourced data can feed discussions about accountability and provide some degree of balance to performance data produced by the people under scrutiny?

Our thought experiment has shown that a multidisciplinary Web Science perspective is essential, combining Philosophy, Computer Science, Network Science, Psychology, Criminology and even Behavioural Economics in exploring varying types of knowledge of crime in a knowledge economy. Through combining these perspectives and theoretical approaches we could create new architectures to shape the spaces of crime and crime reporting. This could help build up society's knowledge of crime. This feeds technologically strategic decision-making on crime policy, and discussions on crowdsourcing accountability data to offset statistics generated by those under scrutiny.

But how far are our current conceptualisations going to take us when we consider the impacts of such technologies? How can we *do justice* – either to victims, or to the problem of defining large-scale human phenomena such as massed goals and intentions in a space as sensitive as that of reporting crime, abuse or violence? The reduction of these phenomena to nodes and edges in network, risks losing the essence of the responsibilities – legal, ethical and social – of such a social machine. The unintended consequences of implementing a machine that attempts to "fight crime" are likely to be unacceptably high unless we consider the

[6] See Acknowledgements for more information on the Group.

ramifications of technology attempting to solve problems of "social constraint" in more depth.

6. ACKNOWLEDGEMENTS

The work in this paper was funded by the Research Councils UK Digital Econony Programme, Web Science Doctoral Training Centre, University of Southampton, EP/G036926/1 and by SOCIAM: The Theory and Practice of Social Machines, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/J017728/1 comprising the Universities of Southampton, Oxford and Edinburgh. The work refers to an application developed at KAIST, in South Korea by Kyoung-Won Lee, (kyongwon.lee@islab.kaist.ac.kr) in the Division of Web Science Technology, Dong-Wan Choi, in the Department of Computer Science (dongwan@islab.kaist.ac.kr) and Chin-Wan Chung (chungcw@kaist.edu) in both departments.

7. REFERENCES

[1] An overview of sexual offending in England and Wales: 2013. *http://www.justice.gov.uk/statistics/criminal-justice/sexual-offending-statistics*. Accessed: 2013-03-21.

[2] Apps Against Abuse: 2012. *http://appsagainstabuse.challenge.gov/*. Accessed: 2013-02-28.

[3] Berners-Lee, T. and Fischetti, M. 1999. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. Orion Business Books.

[4] Clegg, H. 2007. Evolutionary Psychology. *Mapping Psychology*. D. Miell et al., eds. Open University Press.

[5] Crowdsourcing tools to combat violence against women: 2012. *http://tech2.in.com/features/web-services/crowdsourcing-tools-to-combat-violence-against-women/661842*. Accessed: 2013-02-14.

[6] Crowdsourcing.org: 2012. *www.crowdsourcing.org*. Accessed: 2013-02-28.

[7] Ericson, R. and Haggerty, K. 1997. *Policing the Risk Society*. Clarendon.

[8] Futuyma, D. 2009. *Evolution*. Sinauer Associates.

[9] Hendler, Jim; Berners-Lee, T. 2009. From the Semantic Web to social machines: A research challenge for AI on the World Wide Web. *Artificial Intelligence*. (2009).

[10] Hoyle, C. 2000. Police Response to Domestic Violence. *British Journal of Criminology*. 40, 1 (Jan. 2000), 14–36.

[11] O'Hara, K. 2013. Social Machine Politics Are Here to Stay. *IEEE Internet Computing*. 17, 2 (2013).

[12] O'Hara, K. and Hutton, W. 1994. *Trust*. Icon Books.

[13] Opinion Matters 2010. *Wake Up To Rape Research Summary Report*.

[14] Reporting of Sexual Violence Incidents: 2010. *http://www.nij.gov/topics/crime/rape-sexual-violence/rape-notification.htm*. Accessed: 2013-02-13.

[15] Robertson, D. and Giunchiglia, F. 2013. Programming the social computer. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 371, 1987 (Feb. 2013), 20120379–20120379.

[16] Shadbolt, N. et al. 2013. Towards a Classification Framework for Social Machines. *The Theory and Practice of Social Machines* (2013).

[17] Tarling, R. and Morris, K. 2010. Reporting Crime to the Police. *British Journal of Criminology*. 50, 3 (Mar. 2010), 474–490.

[18] The Islington Crime Survey: 1996. *http://www.bunker8.pwp.blueyonder.co.uk/misc/ics.htm*. Accessed: 2013-02-21.

[19] Tierney, J. 1996. *Criminology Theory and Context*. Pearson Education Limited.

[20] Turing Machines: *http://plato.stanford.edu/entries/turing-machine/*. Accessed: 2013-02-14.