"Tool Clinics" – Embracing Multiple Perspectives in Privacy Research and Privacy-Sensitive Design

Anthony Morton[1], Bettina Berendt[2], Seda Gürses[2], and Jo Pierson[3]

[1] University College London, UK; [2] KU Leuven, Belgium; [3] Vrije Universiteit Brussel, Belgium

Last draft. To appear in A. Acquisti, I. Krontiris, M. Langheinrich, & A. Sasse (Eds.), *My Life, Shared - Trust and Privacy in the Age of Ubiquitous Experience Sharing*, Dagstuhl Reports, vol 3, issue 7, 2013.

Focalism – The Challenge

Computer scientists or engineers are continually asked to "solve problems" or "improve" existing situations, by selecting from available design features to produce the "best" technical solution. For example, a software developer faced with the problem of securing data must choose between different encryption algorithms – each with different characteristics. Factors such as strength of encryption, speed of encryption, usability, key management and hardware requirements must all be considered. Other requirements such as the sensitivity and amount of data to be protected, the estimated resources of potential attackers, the operational context of the required solution, etc. must also be taken into account. It is impossible for any solution to be 100% perfect, e.g. encrypting data with no detectable delay using an algorithm which cannot be broken. Trade-offs during the design and development process are therefore inevitable as requirements are balanced, e.g. speed *vs.* strength of encryption. These trade-offs are dilemmas faced by the specialist in arriving at the final design. However, what is the "best solution", and who decides what "best" means, requires more involved discussion and reflection. The engineer, with their narrow focus on solving the technical problem, might not be best equipped to solely decide what the optimum solution is, particularly if there are likely to be unintended consequences when the solution is deployed, or the proposed technology is decoded differently by users, those directly or indirectly affected, and other stakeholders.

The desire of specialists – particularly those in the fields of science or technology – to frame complex and messy situations as a single problem to be solved by technology – for which only they have the answer – often leads to overconfidence in the envisaged solution, an overemphasis on intended consequences, and a tendency to focus narrowly on one or a few aspects of the problem. This is typically identified as a form of "technological determinism", a perspective which consists of two parts: (1) the belief that technological developments take place outside society, independently of social, cultural, economic and political forces; and (2) the assumption that technological change causes or determines social change [13]. This kind of technologically deterministic approach can result in bigger problems than the one originally being solved because the understanding of the original problem situation was incomplete or wrong; Tenner [27] calls these the "unintended consequences" of technological innovation, e.g. the increasing resistance of certain strains of bacteria to antibiotics. However, unintended consequences are not restricted to technological innovation, but occur in political science, organisations, medicine and public health, ecology and social systems [10, 27]. Ehrlinger and Eibach [10] observe:

> "[F]*ocalism, or a tendency to focus narrowly on one or a few variables,* [...] *with respect to the intended consequence can result in a neglect of important information regarding alternative, unintended consequences – including information that is knowable and plainly relevant to predictions*" (p.60)

Using a computer simulation, Ehrlinger and Eibach [10] showed that participants who were "defocused" by being encouraged to consider a wider system of variables, tended to make more accurate predictions and were less optimistic about the proposed solution. This suggests that viewing problems more holistically – particularly from multiple perspectives – can improve decision-making and increase the chances of successful technology development. Focalism – probably first suggested by Wilson *et al.* [31] – is essentially the same as "focusing illusion" proposed by Schkade and Kahneman [23] and Loewenstein and Schkade [15]. They found that when people are asked to predict their emotive reaction to a major event (e.g. the loss of employment), they typically

concentrate on their likely responses to the focal event, to the exclusion of possible effects of other non-focal events (e.g. new opportunities to start a business or retrain). A practical example of people's tendency to ignore other events when their attention is focused elsewhere – inattentional blindness – is described the study by Simons and Chabris [24] in which most people missed a gorilla appearing during a video, when asked to concentrate on the number of times the ball was passed between particular basketball players.

We propose that the notion of focalism is equally applicable to scientists and technologists, who are often reluctant to challenge assumptions surrounding a problem, and principally concentrate on finding a solution to the problem as they perceive it, without adequate consideration of: (1) what it is that actually needs to be achieved – not from only one viewpoint; (2) any foreseeable consequences of the proposed solution; (3) and the viewpoints of other affected and/or interested actors who may have different priorities. We suggest this can be viewed as "solution focalism", and we propose that de-focusing may best be achieved by making other viewpoints salient As Genus observes, "*the employment of participatory approaches has been proposed to accommodate the interests of a wide range of actors holding different value positions, while minimising the potential risks associated with technology development.*" [11]

The problems of focalism are not restricted to technology development. It also reduces the efficacy of privacy research and privacy-sensitive design. For example, Privacy Enhancing Technologies (PETs), such as Privacy Bird and Privacy Finder[1], appeared *prima facie* at the time to offer useful technical solutions to the problem of managing people's privacy. Both PETS use a protocol published in 2002 by the Platform for Privacy Preferences Project (P3P) [9] that enables web sites and applications to describe their privacy policy in XML. However, they have failed to become widely accepted and deployed. In 2003, the adoption rate of P3P was broadly flat at around 10% [6], partially due to the limited functionality of the first P3P user agents, and user interface problems [7]. Reay *et al* [20] observed that "*P3P adoption has stagnated in a niche position; it appears that browser implementers simply do not have enough market incentive to expend the resources needed to develop and integrate P3P 1.1 user agents*" (p.162). Those browser implementers that did implement P3P made such fundamental technical mistakes that P3P was easily circumvented by publishing invalid policies [8]. Companies who chose not to use P3P suffered no consequences, which underlined the fact that P3P – albeit an elegant technical design – also required, as a minimum, enforcement external to itself, either through government regulation or industry self-regulation, both of which never materialised. The development of P3P may have benefited from collaborative design and development informed by a critical assessment of the perspectives of browser developers, the interests and technical capabilities of those who host and manage web sites, and the role of regulators. Certainly, there is much to be learned from the P3P experience that can be used to look at contemporary proposals for privacy-sensitive design. Focalism has also influenced the empirical aspects of privacy research. Many privacy studies have focused on the user experience with different interfaces and privacy controls, without thinking more holistically and considering the context in which the tool is used, the primary goals the user is trying to achieve, or the interaction of these goals with the interests of other affected stakeholders.

We propose a "tool clinic" to encourage a collaborative (re)consideration of a technological solution, research technique or other artefact, in order to critically assess its design, development and deployment from multiple perspectives. Another objective is to turn such solutions or artefacts into a tool for exploring the problem space. For example, what is the privacy problem when we look at it through a solution such as P3P? Finally, a tool clinic can be used to provide those who are developing the solutions with a setting to rethink the framing and presentation of their solutions. The term "tool clinic" emphasizes the motivation for embarking on this exercise. Athletes dedicated to improving some specific skill routinely go to a "rebound clinic" (in basketball) or a "dribbling clinic" (in football). The use of the word "clinic" does not indicate that a tool clinic provides a specific fix for problems, best practice guidelines, or solution templates –a typical panacea sought by those in the field of engineering. Rather, a tool clinic provides a framework and approach for multiple-perspective formative exploration and review of a technological solution, research technique or other artefact under development. The objective is to reflect from different perspectives on practices around the development, encoding, use, domestication, decoding and sustainability of a tool to gain quasi-ecological validation. In this sense, a tool clinic is more like a "law clinic", where law students study law and practice the adversarial legal process in context, or "design crits", during which designers learn to critique and receive critique of their work from others in the arts, academia or design practice.

[1] Privacy Bird was initially developed by AT&T. Privacy Bird and Privacy Finder are managed by Carnegie Mellon University's Usable Privacy and Security Laboratory. See http://cups.cs.cmu.edu/ for further information.

Existing Uses of Multi-perspective Formative Exploration and Review

It is important to demonstrate that similar approaches to the suggested "tool clinic" are already used successfully in areas of industry and academia. This section describes some existing techniques that use a multi-perspective and collaborative approach.

In industry, disaster recovery practitioners often use corporate "war games" – a term originating from the military – to simulate a potential disaster situation (e.g. the loss of a data centre), and step through its disaster recovery plans to ensure they operate correctly. This avoids situations such as employees not being able to relocate to a cold-standby office building due to keys or swipe-cards not being readily available because the security department was excluded from disaster recovery planning. The use of disaster recovery simulations involving all affected areas of the business ensures disaster recovery plans are considered from multiple perspectives. A related technique to war games, the "Red Team"[2] review, also originated in the military as a means of assessing plans in an operational context from the perspectives of adversaries, affected areas of the military and their partners. Like war games, a Red Team review subjects a problem, plan, process, technique or artefact (e.g. tool, document, service, software product, etc.) to rigorous scrutiny by trained team members and experts. One of the authors of this report has been involved in Red Team reviews of complex commercial bid documents by the technical design and implementation, financial, service management and legal areas of a business organisation.

Gaining multiple perspectives is a technique also used by Soft Systems Methodology (SSM), which emerged in the 1980s from Checkland's work [4, 5]. SSM is a framework for organising the exploration of messy, complex problems as a learning *system*, and therefore failures in projects, processes etc. are viewed as a *systems failure*. Checkland [4] suggests that to fully understand a system it is necessary to consider its purpose from different viewpoints. This systemic pluralism represents one aspect of the "soft" systems approach, which aims to construct a rich picture of a problem, encompassing different viewpoints, rather than the reductionist focus of systems engineering. These different viewpoints, or *Weltanschauungen*, represent unquestioned models of the world that makes the system meaningful for study [4, 5]. It is important to stress that although SSM views problems as a *system*, it is not a representational model of reality; it is epistemological, not ontological; just because SSM views a situation *as if it were* a system, does not mean *it is* a system [5], e.g. a computer system.

To facilitate understanding of the reasons for failures, Checkland created the idea of a *formal system model* (FSM), which is a "*general model of any human activity system*" [4]. Comparison between the formal system model and the conceptual model of the problem situation under investigation is an intrinsic part of the SSM process, as it identifies flaws, weaknesses and omissions in the conceptual model, facilitating its improvement. The improved conceptual model can be compared with the real-world situation to determine which desirable or feasible changes are required [4, 5]. A project specific form of the FSM has been developed by Fortune *et al* [29] for use in analysing project failures, such as large-scale building projects [30].

The existing multi-perspective techniques described thus far, not only subject items to rigorous review, but encourage collaborative improvement and design. Soliciting the viewpoints of stakeholders, potential users of a technology or service, and those affected by it, can dramatically improve its quality. The notion of collaborative development and improvement to ensure effort is not expended on features or services that customers do not require, is key to the notion of "*the lean startup*" [21] used by many Internet companies. The lean startup philosophy suggests that companies release a "minimum viable product" – a "*version of a new product which allows a team to collect the maximum amount of validated learning about customers with the least effort"* [21] – to a subset of sympathetic customers, such as early adopters. The release of a minimum viable product is part of an iterative prototyping process, collecting suggestions for improvement, learning how customers use the product and what they want from it. The use of minimum viable products allows business to understand how customers actually decode the technology or service being provided; the product must be viable in that the customer must value what it provides. Use of minimum viable products should be an iterative learning process, generating ideas and collecting data about product use.

One existing approach to answer the question posited earlier, "*Who decides what 'best/better' really means?*" is constructive technology assessment (CTA). The latter fits within the long-standing tradition of Science and Technology Studies (STS), which investigates how the things that it studies are being constructed.

[2] A "Red Team" is defined as "*a team that is formed with the objective of subjecting an organisation's plans, programmes, ideas and assumptions to rigorous analysis and challenge. Red teaming is the work performed by the red team in identifying and assessing, inter alia, assumptions, alternative options, vulnerabilities, limitations and risks for that organisation.*" [28].

The STS domain has increased its scope over the years, starting with scientific knowledge and expanding to artefacts, methods, materials, observations, phenomena, classifications, institutions, interests, histories, and cultures [25]. One of the most prominent ways to apply the thinking in STS in the real world has been the CTA approach. The objective of CTA is to "*produce better technology in a better society*" [11] by taking a more social constructionist position, and moving "*beyond technological determinism towards an evolutionary view of technology development*" [11]. This is done by advising on interventions in early stages of technology development based on the assessment of possible problems and risks that these technologies could pose for society [26]. CTA emphasises the importance of including a wide range of actors to anticipate the potential impact of a technological development ("vermaatschappelijking" of technology [16]) and decide on improvements to it, thus facilitating social learning. It should be stressed that CTA is not a research method, but an overall approach into which participatory techniques may be placed. Genus [11] suggests moving away from the interventionist and prescriptive stance of existing CTA approaches towards a more discursive, democratic and reflective process because "*contention and openness to criticism are prerequisites for producing reflective socio-technical expertise*" [11]. This is also known as "participatory technology assessment" [14]. The use of a modified form of CTA to address the ethical problems caused by technology is proposed by Palm and Hansson [18] as part of a continuous dialogue between developers and affected actors. For emerging technologies, Merkerk and Smith [16] propose a three-step CTA approach, using permutated dialogue workshops attended by insiders and outsiders to the item under review to consider selected issues about the proposed technology and reflect on different technology scenarios.

In order to apply multi-perspective formative exploration and review of technological solutions or tools in early stages of development, different types of multi-method approaches have been developed. One of the most elaborate ones is the living laboratory approach. The 'living lab' is a specific type of test and experimentation platform (TEP), which refers to facilities and environments for (joint) innovation including testing, prototyping and confronting technology with usage situations [2]. Living labs are facilities for designing, developing, testing and evaluating communication technologies and services in early stages of the innovation process. They do so by involving (early) users, in line with the CTA perspective. However they can also be configured as open and innovation-oriented platforms that involve various technology experts, disciplines and/or stakeholders in different stages of technology design, development and testing [19]. Thus, we discern three main ways to put living labs[3] into action as: (1) a platform for open innovation; (2) a user-driven research methodology; and (3) an experimental setting [22].

Perceived Research Gap in Privacy

Most privacy researchers agree that privacy is contextual, and dependent upon information use, information sensitivity and the trust in the entity collecting, storing, processing and disseminating the information entrusted to it [1]. Furthermore, users engaged in technology mediated interactions with other parties will have expectations and assumptions about the technology, the providing organisation and other partners in communication [1].. If these are assumptions and expectations are violated, the user is likely to have an emotional reaction and reject the technology and/or providing organisation [1]. A practical example of this was the launch of Google Buzz. Gmail users believed they were only signing onto Gmail as usual, when they were actually being enrolled in Google Buzz [12]. It would appear the developers of Buzz did not take account:(1) that peoples' primary task was to access their e-mail and hence they would likely "swat away" any dialogue boxes without properly reading them; and (2) that peoples' mental model is that Gmail is a tool to access their e-mail and not a social networking service.

User studies may aid developers and designers in foreseeing likely troubles that users may have with a given design. However, the task of achieving an understanding of the complexity of the privacy problem, and translations of this problem into the technical solution space may benefit greatly from a multi-perspective approach. This is line with the notion of *contextual integrity* (CI) by Nissenbaum [17], which is used to answer whether a situation contained a privacy breach or not. CI is guided by norms of appropriateness (i.e. norms that govern what can be disclosed in a certain context or situation) and norms of distribution (i.e. norms which assess the transfer of personal information from one party or context to another context). This demonstrates how not all publicly revealed information or information collected in the public space, is meant for every form of public use. *"Just because something is publicly accessible does not mean that people want it to be publicized. Making something that is public more public is a violation of privacy."* [3]

[3] In Europe living labs are associated in the European Network of Living Labs (ENoLL) which was set up under the auspices of the Finnish EU presidency in 2006 and since the 6th wave of call for new members in March 2012 consists of over 300 accepted members (http://www.openlivinglabs.eu).

Addressing the privacy implications of increasingly complex, powerful and ubiquitous computing will be even more of a challenge than Buzz, as the potential for unintended consequences is even greater than before. However, privacy researchers and practitioners continue to work largely in isolation, concentrating on people's use of different user interfaces for privacy control, and have largely ignored existing cross-disciplinary collaboration techniques such as those described in the first section.

Future Directions for Researchers and Practitioners

Tool clinics are essentially practices, and they need to be living practices – thus future directions are not only researching, but also must be *doing* tool clinics. We have performed a first *ad hoc* requirements analysis for tool clinics at the Dagstuhl Seminar itself (i.e. we "clinicked" the tool clinic idea) and have seen the challenges the concept poses. Most importantly, our clinic participants expressed concerns about exposing their methods, approaches and original ideas to a critical audience. Further issues were raised with respect to matters of intellectual property. Some of these problems are likely to stem from the employment requirements and the working conditions of senior and junior researchers. They also often associated the world "clinic" with doctoring their (software) artefacts with others, a goal that we only partially share.

Based on this experience, our next step will be to develop a tool clinic as a new event format for a scientific conference, ideally at a renowned computer-science conference. This will combine the tool-centric nature of a demo session, the protected space of work-in-progress afforded by a workshop, and the mentoring spirit of a doctoral workshop.[4]

The format of a tool clinic session could typically consist of three steps (inspired by the CTA and Privacy by Design approach):

1. Identifying particular affordances of the technological solution, research technique or other artefact and possible (unintended) consequences for people and society;
2. Gathering perspectives and practices of different experts, disciplines and/or stakeholders (e.g. users, policy makers, industry, etc.) linked with the development, deployment and sustainable evolution of a particular tool, solution, technique or artefact;
3. Informing and advising on technological design of the tool or solution, in order to avoid negative consequence and to further positive outcome.

We foresee three essentially needed incentives for participation: (1) enlisting big names in the field who can signal through their own example that "grown-ups too can learn"; (2) a broad-enough team of participants to represent a wide range of perspectives; and (3) a follow-up that makes it worthwhile to put oneself into the ring. For the first two, we can draw on our respective scientific networks. A special issue in a good journal is one option for creating the third incentive, and further developments of the tool clinic method described in the introductory article of this special issue is also one of the next intended research activities.

References

[1] Adams, A. and Sasse, M.A. 2001. Privacy in Multimedia Communications: Protecting Users, Not Just Data. *Human-Computer Interaction* (2001).

[2] Ballon, P. et al. 2007. Fostering Innovation in Networked Communications: Test and Experimentation. *Designing for Networked Communications: Strategies and Development*. (2007), 137.

[3] Boyd, D. 2010. Making sense of privacy and publicity.

[4] Checkland, P. 1981. *Systems Thinking,Systems Practice*. John Wiley and Sons, Chichester.

[5] Checkland, P. and Scholes, J. 1999. *Soft Systems Methodology in Action: Including a 30 Year Retrospective*. John Wiley & Sons Ltd., Chichester.

[6] Cranor, L.F. et al. 2003. *An Analysis of P3P Deployment on Commercial, Government, and Children's Web Sites as of May 2003*. AT&T Research Laboratories.

[7] Cranor, L.F. 2003. P3P: Making Privacy Policies More Useful. *IEEE Security & Privacy Magazine*. 1, 6 (Nov. 2003), 50–55.

[8] Cranor, L.F. 2012. The Economics of Privacy: Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *J. on Telecomm. & High Tech. L.* 10, (2012), 273–445.

[9] Cranor, L.F. 2002. *Web Privacy with P3P*. O'Reilly Media.

[4] In this way the tool clinic approach has some resemblance with a 'crit' as done in art schools. This is a critique session, in which a student's artwork is formally presented to and evaluated by a group of faculty and peers, responding with feedback: comments, questions, advice, cheers, jeers, and tears. (http://retnull.com/index.php?/texts/the-crit)

[10] Ehrlinger, J. and Eibach, R.P. 2011. Focalism and the Failure to Foresee Unintended Consequences. *Basic and Applied Social Psychology*. 33, 1 (2011), 59–68.
[11] Genus, A. 2006. Rethinking constructive technology assessment as democratic, reflective, discourse. *Technological Forecasting and Social Change*. 73, 1 (Jan. 2006), 13–26.
[12] Google Buzz "breaks privacy laws:" 2010. *http://news.bbc.co.uk/1/hi/technology/8519314.stm*. Accessed: 2013-06-18.
[13] Hackett, E.J. and Society for Social Studies of Science 2007. Technological determinism is dead; long live technological determinism. *The Handbook of Science and Technology Studies*. MIT Press, Published in cooperation with the Society for the Social Studies of Science.
[14] Joss, S. and Bellucci, S. 2002. *Participatory technology assessment: European perspectives*. Centre for Study of Democracy, University of Westminster.
[15] Loewenstein, G. and Schkade, D. 1999. Wouldn't it be nice? Predicting future feelings. *Well-being: The foundations of hedonic psychology*. (1999), 85–105.
[16] Van Merkerk, R.O. and Smits, R.E.H.M. 2008. Tailoring CTA for emerging technologies. *Technological Forecasting and Social Change*. 75, 3 (Mar. 2008), 312–333.
[17] Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
[18] Palm, E. and Hansson, S.O. 2006. The case for ethical technology assessment (eTA). *Technological Forecasting and Social Change*. 73, 5 (Jun. 2006), 543–558.
[19] Pierson, J. and Lievens, B. 2005. Configuring living labs for a "thick"understanding of innovation. *Ethnographic Praxis in Industry Conference Proceedings* (2005), 114–127.
[20] Reay, I.K. et al. 2007. A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future. *IEEE Transactions on Dependable and Secure Computing*. 4, 2 (2007), 151–164.
[21] Ries, E. 2011. *The lean startup: how constant innovation creates radically successful businesses*. Portfolio Penguin.
[22] Sauer, S.C. 2013. User innovativeness in living laboratories: everyday user improvisations with ICTs as a source of innovation. (2013).
[23] Schkade, D.A. and Kahneman, D. 1998. Does Living in California Make People Happy? A Focusing Illusion in Judgments of Life Satisfaction. *Psychological Science*. 9, 5 (Sep. 1998), 340–346.
[24] Simons, D.J. and Chabris, C.F. 1999. Gorillas in our midst: Sustained inattentional blindness for dynamic events. *Perception-London*. 28, 9 (1999), 1059–1074.
[25] Sismondo, S. 2008. Science and Technology Studies and an Engaged Program. *The Handbook of Science and Technology Studies*. E.J. Hackett et al., eds. The MIT Press.
[26] Smit, W.A. and Oost, E.C.J. 1999. *De wederzijdse beïnvloeding van technologie en maatschappij: een Technology Assessment-benadering*. Coutinho.
[27] Tenner, E. 1997. *Why things bite back: technology and the revenge of unintended consequences*. Vintage Books.
[28] UK Ministry of Defence 2013. *Red Teaming Guide (2nd Edition)*.
[29] White, D. and Fortune, J. 2009. The project-specific Formal System Model. *International Journal of Managing Projects in Business*. 2, 1 (2009), 36–52.
[30] White, D. and Fortune, J. 2012. Using systems thinking to evaluate a major project: The case of the Gateshead Millennium Bridge. *Engineering, Construction and Architectural Management*. 19, 2 (2012), 205–228.
[31] Wilson, T.D. et al. 2000. Focalism: a source of durability bias in affective forecasting. *Journal of personality and social psychology*. 78, 5 (2000), 821.