



8-1-2013

Is Security Sustainable?

Jeremy W. Crampton

University of Kentucky, jcrampton@uky.edu

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Follow this and additional works at: https://uknowledge.uky.edu/geography_facpub

 Part of the [Geology Commons](#), [Information Security Commons](#), and the [Science and Technology Studies Commons](#)

Repository Citation

Crampton, Jeremy W., "Is Security Sustainable?" (2013). *Geography Faculty Publications*. 17.
https://uknowledge.uky.edu/geography_facpub/17

This Commentary is brought to you for free and open access by the Geography at UKnowledge. It has been accepted for inclusion in Geography Faculty Publications by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Is Security Sustainable?**Notes/Citation Information**

Published in *Environment and Planning D: Society and Space*, v. 31, issue 4, p. 571-577.

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 3.0 License (<http://www.creativecommons.org/licenses/by-nc/3.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page(<http://www.uk.sagepub.com/aboutus/openaccess.htm>).

Digital Object Identifier (DOI)

<https://doi.org/10.1068/d3104com>

Commentary

Is security sustainable?⁽¹⁾

Writing in these pages over a decade ago, I suggested that there are “risks of security” (Crampton, 2002). What I meant by that was that security was not necessarily an unalloyed good, despite its prevalence in the aftermath of September 11, 2001. The title was a bit of a pun, of course, since security is by definition the management of risk. There were two ways I thought that security itself might pose risks. On the one hand, processes of security might have a tendency to treat people and things as objects that could be calculated against some normative ideal. The purpose of this would be to more easily perform political governance by the state. On the other hand, security practices might be turned inward within the homeland, and therefore give rise to increasing surveillance and tracking. In other words, security is reductionist and it penetrates the fabric of daily life.

How has security fared as a term of critical analysis since then? Nowadays it is not too surprising to hear of insecurities alongside security. Usually this refers to a lack of sufficient security (eg, food or job insecurities), with the assumption that security can be bettered if its gaps or weaknesses can be properly identified. But there is also now a significant body of work attempting a critique of security per se (Bigo and Tsoukala, 2008; Neocleous, 2008). This work roughly corresponds to my first point: that security is a technology of government and as such is about power. Or to put it another way: security for somebody is always insecurity for someone else.

More recently, Neocleous and Rigakos (2011) have issued a declaration of “anti-security”. They go further still than the above points and claim that security is a dangerous illusion and fetish, a false consciousness that diverts attention away from exploitation and alienation. They offer several reasons for this, a couple of which are particularly interesting to me. First, they claim there is a false choice between freedom and security. Not only are the two terms asymmetrically mismatched, they argue (that is, security always and easily triumphs over freedoms), but they are actually part of the same thing; “liberty has always been security’s lawyer”, as they put it (page 16). It is indeed demonstrably true that in any confrontation between, say, privacy and security, people will substantially prefer security. In a not atypical poll by USA Today/Gallup in November 2010, for instance, when asked whether the loss of their personal privacy is ‘worth it’ as a method to prevent terrorism, 71% of respondents said that it was, and only 27% said it was not worth it. At the same time, about a third of Americans thought that there were health risks to security, for example from the new millimeter wave scanners being introduced to airports. Put these two results together and it is clear that Americans want ‘security’ at either the cost of their personal privacy or their health. The same poll found that majorities of Americans favor governmental profiling to gain security, including of nationality (55% support), “personal appearance” (50% support), “personal behavior” (86% support), and it showed significant support for racial and religious profiling (40% support).⁽²⁾

Neocleous and Rigatos also argue that security diverts attention away from linkages between security and pacification. This is a potentially informative approach, especially

⁽¹⁾ This commentary is an expansion of a piece entitled “The costs of security” that originally appeared on the *Society and Space* Open Site at www.societyandspace.com/2013/06/17/jeremy-crampton-the-costs-of-security

⁽²⁾ See <http://www.pollingreport.com/terror.htm>

their reference to land reform and counterinsurgency. As has been noted, land reform and its technologies such as mapping, geographical information systems (GIS), and cadastral surveys are instrumental in normalizing space and asserting authority over a territory. For very different takes on this, see Demarest (2003) and Lacoste (2012 [1976]).

These viewpoints mark out the opposite ends of the security debate; either it is an assumed good, or an assumed ill. Neither approach, however, puts security to work in the service of something more fundamental, namely assessing security on the basis of human well-being. Can we have a sustainable security?

We might begin by asking what indications there are that privacy has been fatally compromised by security in the long run. Will we regain lost privacy protections? Or, once gone, are they gone forever? I don't know of a way to consensually answer that question—essentially one of the resilience of privacy—at this time. The question is made more difficult if privacy is understood as a practice rather than a quantifiable (and hence more easily measurable) thing we can possess to varying degrees.

The question is more easily posed in the short term. Consider the following: the single easiest way to be tracked and surveilled is to carry an always-on device with you that frequently connects to detectors which log your location and other activities in real time. The data from this device can then be stored and if necessary made available to others, including governments and law enforcement agencies. This device is more commonly known as a mobile phone, and there are now about six billion people with access to one. Smartphones, which usually have additional locational capabilities such as GPS, are growing at an annual rate of 44%, and according to one study there will be about 1.5 billion of them in use by the end of 2013.⁽³⁾ Some 1.3 million law enforcement requests were made to Verizon and AT&T in 2011 in connection with ongoing investigations (Lichtblau, 2012) seeking subscriber data, including caller locations and the content of conversations.

Mobile phones are of course sold by private companies, rather than directly by the government. In principle, these records are private. (The law varies in the degree of privacy protection, and in today's globalized world a law in one jurisdiction can apply to people outside that jurisdiction if it is distributed there.) But privacy law has usually proved no obstacle for government, including the Obama administration in the USA. If conversations can be plucked in real time from the air by the National Security Agency (NSA) (as Colin Powell famously demonstrated during testimony to the United Nations in 2003), or collected at AT&T switching stations (Singel, 2006), government can also secretly get phone records as they occur, sometimes without informing the phone company, never mind the customer. Current US law, including the USA PATRIOT Act, provides legal authority for these actions. (Phone companies that worked with the Bush administration's warrantless wiretap program were given retroactive immunity by Congress with the approval of the Obama administration.)

Two recent cases in the United States indicate how routine mass communication surveillance has become. In one case it was revealed that the Department of Justice had secretly obtained phone records of editors and journalists from the Associated Press, in this case through a subpoena rather than a probable-cause supported warrant signed by a judge (Sherman, 2013).

In another case, in a series of scoops about the NSA, *The Guardian* newspaper obtained for the first time a copy of an actual court order requiring a telecommunications company to provide transactional "metadata" including location, phone numbers of who was called, and length of call (Greenwald, 2013). The order, which was classified TOP SECRET//SI//NOFORN⁽⁴⁾ was issued by the Foreign Intelligence Surveillance Court, operating under

⁽³⁾ See <http://venturebeat.com/2013/02/06/800-million-android-smartphones-300-million-iphones-in-active-use-by-december-2013-study-says/>

⁽⁴⁾ Top Secret is the highest general level of government classification. SI refers to communication-related intelligence, and NOFORN means the document may not be released to non-US citizens.

the Foreign Intelligence Surveillance Act, and revealed for the first time the scale of the collection. The records of millions of Americans are being collected by the NSA from Verizon, one of America's largest telecoms companies. Unlike records in previous revelations, these records are being collected "indiscriminately and in bulk—regardless of whether [people] are suspected of any wrongdoing" (Greenwald, 2013). They are also no doubt part of a larger collection program; California Democrat senator Dianne Feinstein, who sits on a Senate intelligence oversight committee, said in a press conference on 6 June 2013, that as far as she was aware this was a routine three-month extension of a program going back at least to 2006. Secrecy expert Steven Aftergood commented that "this appears to be a massive overreach by the government, as well as a massive failure of congressional oversight and judicial review to curb the Administration's excess."⁽⁵⁾

The value of cell phone data like these was shown in startling form in the German newspaper *Die Zeit* a few years ago. With the permission of one cooperative customer, Deutsche Telekom made available half a year's worth of his continuous cell-phone data to the paper. *Die Zeit* then enriched this data with other information freely available on the Internet, such as Twitter feeds, blogs, and other social media. The result was a stunningly detailed interactive map showing just what he had been up to ("Friday, 13 November 2009, 5 incoming calls, 5 outgoing calls, total time 0h 28min 20s, duration of Internet connection 5h 18min 5s, 24 outgoing texts").⁽⁶⁾ The map showed where Spitze was at any given time, and even his speed of travel as he passed from one cell phone tower to another.

The *Die Zeit* case might be thought to differ from *The Guardian's* Verizon revelations. In the latter, the court order demanded the so-called 'transactional metadata' and not specific content of the messages. However, it is in the nature of 'big data' that they can be extensively mined for significant patterns and findings, and can be leveraged against ancillary data (Crampton et al, 2013). Telephone metadata are only very weakly legally protected, compared with phone content itself. The reason for this is that you are deemed to have 'given away' metadata, including your phone number and location, and therefore can have no reasonable expectation of privacy. But metadata yield big results—and can be used to garner further surveillance. It was metadata after all that uncovered former CIA Director General David Petraeus' affair with his mistress Paula Broadwell. Investigators were able to note her location and contacts in order to build a case against her before reading any of her messages' content. Investigators then used the metadata as probable cause to obtain a warrant to read her e-mails, which led them to Petraeus (Perez et al, 2012).

Even anonymizing data may not be much help. A recent paper by a team of scholars at the Massachusetts Institute of Technology, Belgium's Université Catholique de Louvain, and Harvard University, examined data for over 1.5 million anonymized cellphone users and found that knowing just four pieces of data was sufficient to uniquely identify 95% of users (de Montjoye et al, 2013). The reason for this is that mobility data are highly unique and even when anonymized do not provide personal privacy. It was also found that decreasing the temporal and spatial resolution did not decrease user identification by that much, implying that even coarse datasets do not provide much assurance of privacy. If this research can be confirmed and extended to other 'spaces' such as that of web browsing, where even an anonymous user can be identified by the browsing path they take, the implications are significant. Geographers have long assumed that "spatial masking", which coarsens or aggregates data (Armstrong et al, 1999), and other forms of anonymization are sufficient to protect privacy. But these methods may have weaknesses that can be exploited to reidentify individuals.

⁽⁵⁾ See <http://blogs.fas.org/secrecy/2013/06/fisc-verizon/>

⁽⁶⁾ The customer was Malte Spitze, a Green party politician. See <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

Let me return from these specific cases of threats to privacy to my original question. Is privacy resilient in the long term? That is, could it keep its essential qualities and recover from these threats? One approach to answering this question consensually is to examine what securities have been bought by the loss of privacy. If it is the case that we are safer now by yielding privacy protections, it may be possible in the future to restore these protections. If on the other hand we are not demonstrably safer, it is likely that privacy protections will continue to be eroded. In other words, what are the costs of security?

The costs of security

Let's stipulate for the moment that geolocational privacy is, if not gone, then well on its way out of the stable. What security have we bought with this loss of privacy? This is a complex question with no easy answer; additionally we need to be clear if we are asking this question for the short or long run.

We could positively answer this question in a number of ways. Below I suggest the most fruitful questions I think we need to ask about the costs of security. We are not close to knowing the answers to these questions, and indeed we have been woefully slow in even asking them. I frame my approach as one of the sustainability of security and the resilience of privacy. Sustainability and resilience have been negative terms for critical thinkers (Neocleous, 2013), but this is often predicated on limited understanding of their implications. Simply put: do our present practices of security irrevocably damage human well-being, including our privacy, health, environment, and democratic principles? If so, what would sustainable security look like?

The first place to begin is to get an estimate on the literal monetary costs of security. What does the US pay? One attempt at an answer to this surprisingly difficult question was recently provided by the National Priorities Project. Their estimate was that the US national security budget was \$1.2 trillion a year (Hellman, 2011). This sum includes all defense spending, including the ongoing wars in Iraq and Afghanistan, homeland security, the US intelligence community (IC), and medical care for veterans, as well as various other related costs. In the financial year 2013, the military in the US will consume about 60% of discretionary federal spending (education will consume about 6.4%). This overall sum remains a rough estimate because many of the details remain classified. For example, beyond the known fact of the requested budget of \$62.8 billion for the IC for the financial year 2014 (excluding overseas contingency funding associated with ongoing military efforts), almost nothing is known about how much, or on what, the intelligence community spends its money.⁽⁷⁾

However—with some effort—it is possible to glean insights into intelligence by examining contracts with private companies, since the latter have to file reports with the Securities and Exchange Commission (SEC), and the federal government posts its bids for contracts publicly. I discuss one of these contracts, with the country's top geographic intelligence agency (the National Geospatial-Intelligence Agency, or NGA) and known as the Enhanced View project, awarded in August 2010 for a total sum of \$7.3 billion over ten years, in a separate paper (Crampton et al, forthcoming).

Other parts of the government's budget are classified, often without good reason. This includes the top-line budget of the core IC agencies such as the CIA, NSA, and NGA. Despite President Obama's promise on the day he took office to head the most transparent administration in history, the reality has been far different. In summary, then, we see here an inverted asymmetry of privacy; it is entirely acceptable for the government to know what we as individuals are doing, but it is not acceptable for us to know much about them. Is the amount and unknown nature of what we spend on security sustainable and consonant with

⁽⁷⁾See <http://www.fas.org/irp/budget/index.html> for the most complete publicly available data on intelligence budgets.

human well-being? I call this an “inverted asymmetry” of privacy because it inverts a clear goal of democracies: that the government should intrude minimally into its citizens’ lives, and that it should be maximally transparent to those citizens.

A second area where we can investigate the costs of security is in the outsourcing of security to the private sector. Following the revelation that the NSA leaker Edward Snowden worked for the defense contractor Booz Allen Hamilton, it has become all too clear what a huge part contractors play in collecting and analyzing intelligence (Shorrock, 2008). According to publicly available data, the Department of Defense (DoD) has spent over \$3.75 trillion in contracts with private companies over the last dozen years.⁽⁸⁾ Over 50,000 different companies have contracts with the DoD, or about one company in every two zipcodes in America. The big GIS company Esri, for example, has taken over \$800 million in government money (about \$437 million from the DoD). Priest and Arkin (2011) call this “an alternative geography of the United States”. Contracting out security causes two problems: security now falls under the profit motive, and oversight is lacking. (As a privately held company, for instance, Esri does not provide reports to the SEC.) But dollar figures are only part of the story here. Personnel from government contractors often rotate into government, and vice versa. This is partly why so many government contracts are awarded on an ‘uncompeted’ basis, or if competed then bid for by only a single company. This practice encourages waste, inefficiency, and malpractice. Director of National Intelligence James Clapper, for example, was an executive at Booz Allen. His opposite number in the Bush administration, Mike McConnell, now works there.

Point three follows from the previous point: increasingly, scholarly research is being enrolled into the securitization agenda, growing the longstanding military–industrial–academic nexus. My alma mater, Penn State, has taken over \$2.8 billion of federal funds (\$2.5 billion from DoD), and my current employer, the University of Kentucky, has taken \$260 million (\$23 million from the DoD). The top university recipient of federal funds is Johns Hopkins which has taken a massive \$9.7 billion, almost all—\$9.1 billion—from the DoD. Interestingly, Harvard, which reputedly has a policy against its faculty doing ‘secret’ research, has taken only \$146 million (\$29 million from the DoD) despite (or because of) its massive \$32 billion endowment. More specifically, an increasing number of universities are now instituting ‘geospatial intelligence certificates’ including George Mason University (one of the country’s most politically conservative universities). These certificates are sometimes set up with intelligence community (ie, DoD) money, and are overseen by an industry group known as the United States Geospatial Intelligence Foundation (USGIF). The USGIF, which had total assets of over \$5 million in the financial year 2011, is in turn largely controlled by defense contractors, and was recently awarded a contract by the NGA to provide ‘special programs’ to enhance the DoD’s mission. The USGIF will also “provide access to schools that have GIS or [geospatial intelligence] academic programs”. Thus there is an increasingly direct link between universities and the state securitization agenda.

Lastly, we can point to much-needed legal reform. In addition to the PATRIOT Act, which has provided the legal authority behind much of today’s surveillance of Americans, there is the forthcoming Cyber Intelligence Sharing and Protection Act (CISPA, or the cybersecurity bill), which the Center for Democracy and Technology found to have eight critical problems rendering it unacceptable. A new version of the Communications Assistance for Law Enforcement Act, which provides legal ‘backdoors’ into telecom and VoIP communications, has been mooted by the FBI, which fears it is “going dark”.⁽⁹⁾ Also on the legal front, it is ironic

⁽⁸⁾ Author’s calculations based on data at usaspending.gov. Note that the NGA received legal dispensation to cease publicly reporting their outsourcing after 2006.

⁽⁹⁾ After the June 2013 NSA revelations, Google strongly denied that for its part it provided any such backdoors, but given other legal authorities, it may not need to.

that the only person prosecuted for torture has been John Kiriakou, the former CIA employee who exposed the practice (in order to defend it), rather than any person who allegedly engaged in torture. Couple this with the Obama's administration's aggressive pursuit of whistleblowers (those who are acting to stop government waste, inefficiencies, and malfeasance) and you have a very troubling legal landscape. Again, we might ask if the 'cost' of this security is worth it, or is even effective in keeping us safer.

In conclusion, we should not be left with the impression that there is nothing that can be done in the face of these grand challenges. As with the case of global climate change (GCC), it is probably insufficient to just have the data on your side; activism will be required. But unlike on GCC we still do not have a consensus on whether or not security is sustainable and leads to positive human well-being. Here are some practical suggestions:

- (1) Challenge the state's presumptive right to knowledge and its inverted informational asymmetries. Matt Hannah has already begun this task in his book *Dark Territory in the Information Age* (2010). In it, he offers a number of prescriptions for how we can rethink collecting data. For example, have citizens and states 'pay in' to 'data producer collectives' reducing the need to classify so many documents (an estimated ninety-two million classifications in the financial year 2011, according to the Public Interest Declassification Board). Regarding classification, when we do examine declassified secrets, they often seem either overclassified (the knowledge of the fact that the Obama administration collects all phone calls does not harm national security) or classified for too long. As Senator Wyden (Democrat, Oregon) has long pointed out, even some of the legal authorities justifying mass surveillance are classified, making the US a nation of secret laws. Recently, the nation's top spy satellite agency, the National Reconnaissance Office, declassified grainy images from the early 1980s of Tyuratam missile base in Baikanur, Kazakhstan. This represents the most up-to-date declassifications of its satellite imagery. A quick comparison with Google Earth, however, shows not only the missile base in superior detail, but the ability to rotate the image, zoom in and out, and apply a three-dimensional landscape. Do we really need to keep these images classified for so long when information in the public domain about them is available?
- (2) Opt-in policies rather than opt-out. Experience shows that opt-in results in far fewer data being collected. For example, Twitter allows users to optionally provide their geolocational information, with the result that only about 1.6% of tweets are geotagged. This is especially critical at the moment of data collection, and implies a much better informed public about how geolocational data are collected. As geographers, we can be part of that process.
- (3) Protect and reward whistleblowers, support information transparency projects such as WikiLeaks and open government data advocates.
- (4) Reduce government outsourcing to for-profit companies, democratize corporate data sharing. Make the scope of contracts public. Require the IC to resume reporting its contracts.
- (5) Legal reform to include warrants (not just subpoenas) for location information. Correct the cybersecurity bill's weaknesses.
- (6) Understand the environmental impacts of security. For example, the anthropologist David Vine estimates there are over 1000 US bases overseas, which he dubs "Baseworld" (2013). Patrick Bigger is one of only a few political ecologists looking at environmental impacts of militarization, in this case the Navy's energy policies on synthetic fuels (Bigger, 2013). More work is desperately needed here.

In sum: understand and promote sustainable security, rather than security for security's sake.

Jeremy W Crampton
Department of Geography, University of Kentucky

Acknowledgements. An initial version of this commentary was given at the annual Center for Geographic Analysis (CGA) conference at Harvard University in May 2013. I thank the CGA, its Director Peter Bol, and Director of GIS Research Wendy Guan for inviting me to participate.

References

- Armstrong M P, Rushton G, Zimmerman D L, 1999, "Geographically masking health data to preserve confidentiality" *Statistics in Medicine* **18** 497–525
- Bigger P, 2013, "Climate change and intra-imperial conflict: the US navy's biofuels purchasing program", paper presented at the annual meeting of the Association of American Geographers, Los Angeles, meridian.aag.org/callforpapers/program/AbstractDetail.cfm?AbstractID=49639
- Bigo D, Tsoukala A, 2008 *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11* (Routledge, London)
- Crampton J W, 2002, "The risks of security" *Environment and Planning D: Society and Space* **20** 631–635
- Crampton J W, Graham M, Poorthuis A, Shelton T, Stephens M, Wilson M W, Zook M, 2013, "Beyond the geotag: situating 'big data' and leveraging the potential of the geoweb" *Cartography and Geographic Information Science* **40** 130–139
- Crampton J W, Roberts S, Poorthuis A, forthcoming, "The new political economy of geographic intelligence" *Annals of the Association of American Geographers*
- Demarest G, 2003 *Mapping Colombia: The Correlation Between Land Data and Strategy* (Strategic Studies Institute, US Army War College, Carlisle, PA)
- de Montjoye Y-A, Hildalgo C A, Verleysen M, Blondel V D, 2013, "Unique in the crowd: the privacy bounds of human mobility" *Scientific Reports* **3** 1–5
- Greenwald G, 2013, "NSA collecting phone records of millions of Verizon customers daily" *The Guardian* 6 June
- Hannah M, 2010 *Dark Territory in the Information Age: Learning from the West German Census Controversies of the 1980s* (Ashgate, Farnham, Surrey)
- Hellman C, 2011, "The real US national security budget" *TomDispatch* 1 March
- Lacoste Y, 2012 [1976] *La Géographie, ça Sert d'abord à Faire la Guerre* (Éditions La Découverte, Paris)
- Lichtblau E, 2012, "Wireless firms are flooded by requests to aid surveillance" *The New York Times* 8 July
- Neocleous M, 2008 *Critique of Security* (McGill-Queen's University Press, Montreal)
- Neocleous M, 2013, "Resisting resilience" *Radical Philosophy* **178** 2–7
- Neocleous M, Rigakos G, 2011 *Anti-security* (Red Quill Books, Ottawa)
- Perez E, Gorman S, Barrett D, 2012, "FBI scrutinized on Petraeus" *The Wall Street Journal* 12 November
- Priest D, Arkin W M, 2011 *Top Secret America. The Rise of the New American Security State* (Little, Brown, New York)
- Sherman M, 2013, "Gov't obtains wide AP phone records in probe" *Associated Press* 13 May
- Shorrock T, 2008 *Spies for Hire: The Secret World of Intelligence Outsourcing* (Simon and Schuster, New York)
- Singel R, 2006, "AT&T sued over NSA eavesdropping" *Wired* 31 January
- Vine D, 2013, "Where has all the money gone?" *TomDispatch* 14 May