NIST NBD-WG Privacy & Security vs. Two White House May 2014 Reports

*Source: NBD-WG Security and Privacy Subgroup*

*Status: Information for Possible Updates for current or future S&P drafts*

*Title: NIST NBD-WG Privacy & Security vs. Two White House May 2014 Reports*

*Author: Mark Underwood, Krypton Brothers*

***Abstract****The White House convened a task force to report on Big Data and Privacy issues. The* [*report was issued*](http://1.usa.gov/1nvL6h9) *in May 2014 as “Big Data: Seizing Opportunities, Preserving Values” (BDSOPV). The purpose of this short list is to identify possible additional issues that the NBD-WG may wish to consider.* [*PCAS*](http://1.usa.gov/1jYh3i5)*T is a parallel report that is somewhat more technical.*

1. The Internet of Things receives a bit more prominent attention in BDSOPV, whereas the NIST draft tends to refer to IoT to support related issues, or as a use case, rather than as a specific concern. The PCAST report specifically calls out “privacy invasion of a person’s virtual home.”
2. BDSOPV addresses the issue of inequity whereas the NIST report does not. “Some of the most profound challenges revealed during this review concern how big data analytics may lead to disparate inequitable treatment, particularly of disadvantaged groups, or create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms.” There is a connection to privacy and security here in that the Digital Divide will create citizens disproportionately able to defend and protect their information. The BDSOPV cites Boston’s StreetBump project as one that tried to address the problem both in the project fielding and information design.
3. BDSOPV addresses so-called MyData initiatives (Blue Button, Get Transcript, Green Button, MyStudentData). These might be worth adding as specific use cases. In the S&P section the NBD-WG draft refers to citizen / user portals as part of provenance and control, but do not offer use cases.
4. Where BDSOPV provides a section for it, the NIST document doesn’t review privacy laws clearly. Perhaps this should be done through a reference or appendix. In particular, the NIST draft may refer to the 2012 White House Consumer Data Privacy Report, which offers a privacy blueprint.
5. The BDSOPV refers to a Council of Advisors [report](http://1.usa.gov/1nvQvon) on controlled access to health information, which may identify possible omissions in the NIST draft. In addition, the BDSOPV refers to a Dept. of Education [initiative](http://1.usa.gov/1kkKqKL) for guidance on online education services. It may be helpful to set up an informal liaison with individuals working on these guidelines, even if it’s just trading drafts.
6. The BDSOPV refers to the DHS pilot programs “Neptune” and “Cerberus.” These could be useful frameworks for NIST readers to review to see how S&P has evolved / is evolving there, albeit in a public project.
7. Should the NIST S&P document have a section called, “Is my system compliant?” which lists possible government (U.S., EU, etc.) executive orders, guidelines, court decisions? It’s a moving target.
8. Segmentation, or “algorithmic data,” as it’s called in BDSOPV, could create system-of-systems data that discriminate – illegally (e.g., redlining violations of the Equal Credit Opportunity Act or Fair Credit Reporting Act) or legally – through customer / prospect segmentation. NBD-WG doesn’t call this out directly.
9. BDSOPV has a section on law enforcement which deals with Big Data for forensics and pattern recognition for detecting human trafficking networks, predictive analytics for repeat offenders (a la *Minority Report*). There’s no corresponding NBD-WG section; it’s only hinted at.
10. BDSOPV calls out the third-party doctrine and *United States v. Warshak*. It quotes Justice Sotomayor’s “concurring opinion that current practices around information disclosure to third parties are ‘ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.’” The NIST draft gives casual attention to opt-out and audit, There’s a discussion of the “notice and consent” framework in BDSOPV: “In the words of the President’s Council of Advisors for Science & Technology, ‘The notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data.’” The NIST document should identify possible solution, either using existing mechanisms, or suggesting new ones. In the PCAST document, this is addressed in more detail, boldly stating that the existing framework is “increasingly unworkable and ineffective.”
11. BDSOPV suggests that current practices around metadata may argue for “more sensitivities” than in previous systems. The report “recommends that the government should broaden that examination beyond intelligence and consider the extent to which data and information should receive legal or other protections on the basis of how much it reveals about individuals.” The BGWG may wish to consider a separate S&P section on metadata disclosure, portals, tracking and audit with some specific use cases and a case study or two. A proposed standard could say as little as recommending that metadata issues be address, or drill into audit and disclosure for PII-based systems. NBD-WG could identify issues or design patterns for metadata catalog, discovery systems.
12. BDSOPV has a chart showing where current privacy funding is going (NSF, etc.). The NIST team perhaps should reach out to some of these principal investigators.
13. Proposed Data Breach and Consumer Privacy Bill of Rights drafts are mentioned in BDSOPV. Any technical or standards notions contained in these draft might be a useful heads-up for Big Data architects --- even if there’s no existing legislation.
14. The [PCAST report](http://1.usa.gov/1jYh3i5) was a parallel White House-requested effort by the Council of Advisors on Science and Technology. It calls out the NITRD agencies to amplify up research and development; there may be potential contact points for S&P. It mentions “trust” implementations in a general way, and calls out ”Palantir and new startups [with] pioneering internal usage auditing, policy analytics, and policy reasoning engines.” The NBD-WG S&P report may want to refer to some of this work, including automated violation detection and notification, transparency frameworks in greater detail than has been done so far.
15. The PCAST report identifies the importance of the Respect for Context and right to Focused [Data] Collection. The NBD-WG doesn’t mention these.
16. PCAST mentions Secure Multiparty computation as a subdiscipline. NBD-WG suggests but doesn’t identify this as a study area for S&P.
17. The PCAST report recommends a focus on practical frameworks,though it’s less clear what these might be. Possibly the NBD-WG S&P should examine how its suggestions could be made more practical (checklists? Case studies – real or hypothetical? Socialization of the existing work? S&P fabric as revealed through its absence – a “difference” filter?).