THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 3 Article 8

9-2017

Security and the Transnational Information Polity

Michael M. Losavio
University of Louisville, michael.losavio@louisville.edu

Adel Said Elmaghraby
University of Louisville, adel@louisville.edu

Recommended Citation

Losavio, Michael M. and Elmaghraby, Adel Said (2017) "Security and the Transnational Information Polity," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 3 , Article 8.
DOI: https://doi.org/10.15394/jdfsl.2017.1458
Available at: https://commons.erau.edu/jdfsl/vol12/iss3/8

Security and the Transnational Information Polity

Cover Page Footnote

We thank the administration and faculty of Perm State National Research University and the City of Perm, Perm, Russian Federation for their efforts and support For the International Symposium on Security of Individuals, State and Society For Which This Paper was written.

SECURITY AND THE TRANSNATIONAL INFORMATION POLITY

Michael Losavio
University of Louisville
Department of Criminal Justice
Louisville, Kentucky, 40292 USA
michael.losavio@louisville.edu

Adel Elmaghraby
University of Louisville
Department of Computer Engineering and Computer Science
Louisville, Kentucky, 40292 USA
adel@louisville.edu

ABSTRACT

Global information and communications technologies create criminal opportunities in which criminal violation and physical proximity are decoupled. As in all our endeavors, the good become the prey of the bad. Murderous and venal exploitation of ICT has followed from the inception of the Internet, threatening all the good it brings and the trust we need so badly as a people. As the work continues to expand the implementation of Smart Cities and the Internet of Things, there will be more opportunities for exploitation of these technologies. We examine the social and liberty risks our data and technology-driven responses may entail.

Keywords: Big data, analytics, privacy, information polity

1. INTRODUCTION

The growth and distribution of internetworked, instrumented objects feeding into an intelligent framework for analysis offer tremendous benefits. These include smart traffic management, smart logistic scheduling, smart policing, smart corrections and all the myriad of services that can benefit from structured, algorithmic analysis and implementation. The growth in analytic power and inference depends on data generated in Smart Cities and the objects of the Internet of Things. With all these benefits we must consider the increased risks of criminal conduct towards personal security and of state overreaching that may shift the balance between state and citizen.

This is particularly true where components of this implement geographic information system analysis. In the game of who-when-where-what-how, the foundation of all investigation and reporting, GIS data can connect the where and when to who and what, either directly or inferentially. The richness of this spatio-temporal data modelling and statistical inference challenges social and legal bounds, especially of

- privacy and
- personal security.

We must consider the systems as a *Socio-Technical* System for Governance and address evolving standards of conduct. And we must consider these for the future as these technologies--- analytics, data generation and data collection ---grow in power.

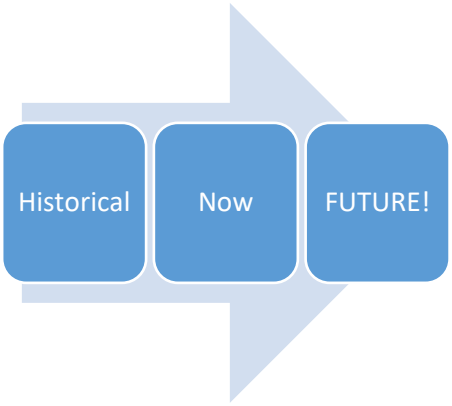

Figure 1. Temporal Considerations for Effective Policy Development

2. LEGAL REGIME OF INFORMATION

One key area are the protections associated with values of privacy and personal autonomy. Both civil and common law have for centuries protected these from intrusion, with doctrines relating to trespass and trespass to chattels up to *sui generis* video voyeurism statutes. This reflects direct invasion of those interests as well as the use of the invasion for other injuries. For example, the United States Congress enacted legislation to prohibit states from selling the information of individuals receiving motor vehicle licenses; although quite profitable for the states, this information was used to stalk, assault and murder the citizens of those states.

These have been issues of policy and law throughout the evolution of informational technologies. For GIS, Onsrud, Johnson and Lopez (1994) observed that personal privacy is a social issue of increasing relevance to the geographic information system community where specific privacy protection practices are needed.

Within the GIS community, Cho (2005) discussed overall legal issues within the data sphere of spatiotemporal information. This examined general law and policy, data sharing concerns, privacy interests and liability for injuries to life, liberty, and property from the application of these technologies. This addressed the impact of jurisdiction (domestic, international, transnational), property interests/intellectual property and contract law within these regimes.

As with issues of governance generally, and with the interaction of new technologies with social life in particular, we begin to see an important and interconnected relationship between research within disciplines of knowledge analysis, the practical use of those

systems and the legal/ethical implications of that use.

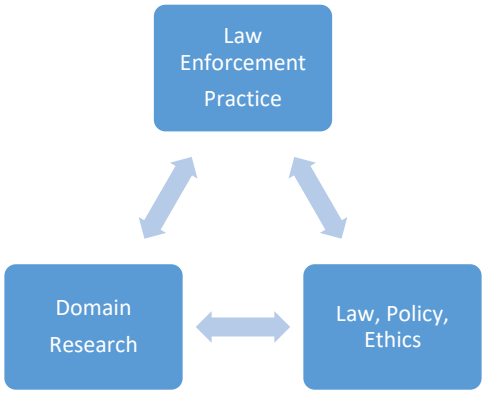

Figure 2 Interrelationship of Research, Practice and Law/Ethics in Polity Governance

These reflect the importance of considering consequences, both historical and potential, the allocation of responsibility for those consequences and the role of governance in balancing the competing interests at issue. They are all interrelated: ethics and outcomes drive policy, which drives political responses which drive legal results which, if not perfect (and they never are) lead to new policies.

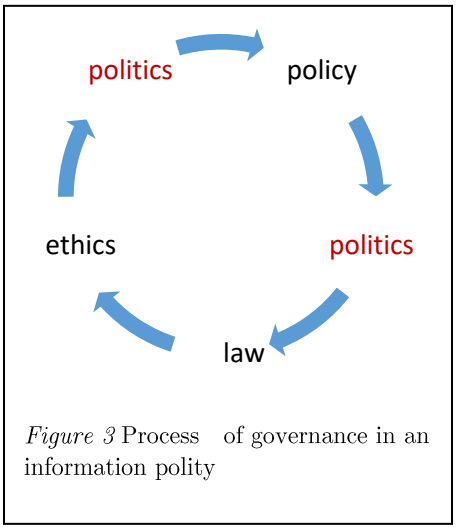

Figure 3 Process of governance in an information polity

2.1 Analysis and Implications under the Laws of the United States

Under American law, no citizen may be deprived of life liberty or property without the due process of law, a constitutional guarantee of fundamental fairness. Issues of due process were discussed in the United States Supreme Court cases of *Goldberg v. Kelly* and *Mathews v Eldridge.* The basic analysis that must take place is a trifold weighing of factors:

1. what is the nature and extent of the injury to the individual by the state action,
2. what is the risk of a wrongful outcome through the use of state action, and
3. what is the nature and extent of the interest of the State in the matter at hand.

The common law's flexibility is essential, for "time works changes, brings into existence new conditions and purposes" *Olmstead v. United States*, (1928) (Justice Brandeis, dissenting). Justice Brandeis wrote a dissent which set the foundation for the subsequent evolution of the law to protect the rights of privacy; his prescient analysis is even more relevant for today:

> Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> Moreover, "in the application of a constitution, our contemplation cannot be only of what has, been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these. ...
>
> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence -- it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence of a crime or to forfeit his goods is within the condemnation of that judgment. In this regard, the Fourth and Fifth Amendments run almost into each other.

Ultimately, the reasoning of Justice Brandeis prevailed and the Supreme Court overruled *Olmstead*, holding that the police interception of telephone calls was a violation of fundamental constitutional protections and an unreasonable search. In that case, *Katz v. United States, (1967)* the Supreme Court further detailed the fundamental test for judging the limits of government power: that a government search is unreasonable in violation of the fourth amendment when it violates a he

reasonable expectation of privacy, thereby moving this doctrine untethered from physical traditions.

This analysis was repeated in a number of 21st-century cases that define privacy interests against intrusion with the evolution of new technologies and new systems. Those cases include *United States v. Jones* (2012), *North Carolina v. Grady* (2015), where satellite monitoring was found to constitute a search under the Fourth Amendment and *Riley v. California* (2015). In *Riley,* cell phone searches incident to an arrest were found in proper, a change from earlier jurisprudence rules which permitted the search of an individual and their possessions once they were arrested. *Riley v. California* reflected Justice Sotomayor's observations in *United States v. Jones* that on GPS profiling power cited in support of the ultimate determination that under the Fourth Amendment there were greater limits on cell phone data searches than for less-data intensive artifacts.

Although the Supreme Court ruled on traditional trespass grounds in *United States v. Jones (2012),* the concurring opinions of Justice Sotomayor, considered a liberal jurist, and Justice Alito, considered a conservative jurist, analyzed the greater, future issues at stake in the growth of these new technologies. Justice Sotomayor noted that *Katz v United States* realigned the controlling test for modern privacy as protecting a person's reasonable-expectation-of-privacy. Her greater concern –a system of inexpensive GIS for people could "alter the relationship between citizen and government in a way that is inimical to democratic society" via GPS data monitoring, aggregation and analysis:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. ...The Government can store such records and efficiently mine them for information years into the future. ... And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois* v. *Lidster*

Justice Alito expanded this analysis as to the instrumented devices contributing data to the geospatial corpus: CCTV, automated tolling systems, automobile automatic notifications systems, cellular telephones and other wireless devices. Joined by three other justices, he suggested that while short-term monitoring would be reasonable, longer-term it would be an illegal invasion of privacy under the Fourth Amendment. As with electronic monitoring of communications, that this was an area open to Congressional legislation to establish privacy rights and the punishments for their violation.

2.2 Legal Analysis for the Future

There are a variety of factors to consider as to the way in which a governance structure within the information polity is rendered. Some of the individual elements that might be considered are:

- Data
- Analytics & Algorithms
- Rendition & Representation
- Systems (collection, storage, analysis, rendition)
- Users and Use/disclosure.

Issues that relate to the individual datum or collected data can be constructed around their characteristics, such as mandates, prohibitions or special permissions on data. This may connect to systems aspects for the generation and collection of data. The use of data analytics and the algorithms which drive such analysis

has generally not been deeply scrutinized except where outputs produce clearly discriminatory results which may conflict with other regulations.

There has been significant discussion about the inherent dangers of discriminatory programming, whether intentional or unintentional, that may produce inappropriate output. This may appear in the final rendition and representation of the data analysis. From this flows issues of who uses that analysis, how they use it or how they might disclose it to others along with any underlying data associated with it.

A number of privacy regimes, such as those of the European Union, distilled this down to three general areas within which regulation is constructed. These general regulatory areas are

1. data collection,
2. data analytics and analysis, and
3. data use and disclosure.

Governance of the potential damage with the use of these systems may seek limitations within these areas and define granular regulations within them.

This intersects with the police power of the state using such powerful data systems to promote public security. These analytics can be used for various types of state action. Limitations on state action vary with national law and, in some cases, the interrelationship with international treaty law, such as those enforced by the European Court of Human Rights. The examination of the implementation of data analytics into police action must consider the different requirements for any particular police action. The continuum of evidentiary weight that each type of police action requires is different for:

- Investigation
- Designation for further contact
- Designation as "person of interest"
- Investigative detention
- P/C
- Arrest
- Search
- Indictment/Prosecution
- Trial
- Conviction

At the same time, there are civil law restrictions on the infringement of personal autonomy that may be based on constitutional provisions, statutes or common-law practices. Liberty and personal autonomy as the rights of the citizens of a polity may look at the right to control access to and distribution of personal information of various types.

The common-law tort of invasion of privacy is instructive in this regard under American law. Where the Second Restatement of Torts set this out as four distinct areas, it captures fundamental areas that can suffer from improper data analytics. Those are:

- The right to be free from the unwarranted appropriation or exploitation of one's personality,
- The publicizing of one's private affairs with which the public has no legitimate concern,
- The wrongful intrusion into one's private activities, in such manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities, or
- Being presented in a "false light."

These areas may be mapped to these technologies and the potential damage they may cause. The publication of aspects of a person's private life with which the public has no legitimate concern or interest may come from analytics which reveal an intensely personal item, such as health, pregnancy or financial frailty, the disclosure of which is harmful and for which there is no need for someone to know. It does not matter if this is a truthful inference,

it's that the disclosure is inappropriate. If made in violation of law that disclosure may lead to related statutory grounds for a privacy invasion.

The privacy tort of "false light" represents another aspect of this, where a mis-inference, or erroneous inference from data analysis may incorrectly represent someone wrongly as to their status, state or conduct and thus injure them in a variety of ways.

Where data analytics allow one to intrude into the private activities of someone, we may have an open question as to what would constitute a wrongful intrusion into that area; violation of statutory limitations on data processing and use that produce this might be such a tortious action. It is possible that a common-law violation may evolve with greater appreciation of the particulars of these new technologies and how they may infringe on one's personal sphere.

And even violation of one's right of "publicity," or the unwarranted appropriation or exploitation of a person's personality, may be violated where mis-inferences are used in connection with disclosures relating to an individual.

The admonition where Justice Brandeis said the right of privacy is the right to be let alone is all the more appropriate. Where data analysis meddles with the lives of others it does not leave them properly alone and society in law may need to correct that.

3. DATA AS A POLITY CONCERN

That this has become a matter of the proper governance of the polity is best seen in the policy white papers issued by the Office of the President of the United States under Barack Obama. In two papers, from 2014 and 2016, the office of the president set out the issues that must be addressed to maintain a proper balance between the government and the government.

The first white paper outlined how "big data," lawfully applied, would have significant benefits for public safety and national security. Yet it acknowledged that its use in these areas, manifested in "predictive analytics," must be regularly subjected to careful policy review as to the outcomes represented. The implementation and institutionalization of "best practices" protocols for data use and storage would be a foundation of this. The White House suggested that engagement of federal agencies with extensive experience in dealing with privacy and data practices could assist state local and other authorities in the proper use of these analytic technologies in accordance with law. This included the use of commercial data products.

The second white paper drilled down into fundamental issues of system design as they related to data analytics for governance. The key challenges that must be addressed relate to the data that is processed by the system, the design of the algorithmic systems (including AI and machine learning technologies), and the way in which this data is used. It noted that these powerful data analytics were used for credit lending decisions, employment decisions, education, healthcare, and criminal justice.

The risks began with data. Where the primary or initial data sets used poorly selected data, incomplete or incorrect data, data tainted by selection bias or internal inferential biases relating to historical practices, improper mis-inferences may be the result of analysis against flawed data. The analytics systems themselves may be subject to inherent problems of evaluation and transparency. They may be "black box" technologies that vendors do not wish revealed or may not themselves fully understand. The systems themselves may have errors within the programming that may produce erroneous outcomes, at least in some situations. This risk is heightened with the growth of self-learning systems of "artificial intelligence" and machine learning algorithms

that may evolve without human intermediation to provide awareness of potential biases or errors. There is a risk the systems will repeat those biases and errors incorporated into past decisions reflected in the data.

4. CONCLUSION

How we balance the risks and benefits of massive data analytic technology will define the relationship between the government and the governed in the information polity, just as Justice Sotomayor said in *United States v Jones.* By failing to address these risks we may very well damage the liberties and democratic engagement we need to continue to be the people we are. This is clearly balanced against the risks of criminal and terroristic actions that threaten the peace and stability of our Republic. But we must address them, and fundamental for this is our willingness to address the impact of these new technologies on our rights and liberties, now and for the future. Failing to do may very well change who we are and who we want to be.

REFERENCES

[1] Onsrud, H.J., J. Johnson, and X. Lopez, "Protecting Personal Privacy in Using Geographic Information Systems", Photogrammetric Engineering and Remote Sensing, 1994, LX(9), 1083-1095

[2] George Cho, Geographic information science: mastering the legal issues, John Wiley & Sons, 2005

[3] Goldberg v. Kelly 397 U.S. 254 (1970)

[4] Mathews v. Eldridge, 424 U.S. 319 (1976)

[5] Olmstead v. United States, 277 U.S. 438 (1928)

[6] Katz v. United States, 389 U.S. 347 (1967)

[7] United States v. Jones, 132 S. Ct. 945, 565 U.S. ___ (2012),

[8] Grady v. North Carolina 575 U.S. ___ (2015)

[9] Riley v. California, 573 U.S. ___ (2014)

[10] Illinois v. Lidster, 540 U.S. 419 (2004)

[11] Executive Office of the President of the United States, Big Data: Seizing Opportunities, Preserving Values (2014)

[12] Executive Office of the President of the United States, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights (May 2016)

