STUDY DLP SYSTEMS AND COMPARE WITH OTHER SECURITY AND DATA PROTECTION APPROACHES

Ravisankar, C.V., Goban kumar, P and G. Addlin Vini

Dept. of Electronics and Communication Engineering
Madha Engineering College, Kundrathur, Chennai- 69, Tamil Nadu, India

ABSTRACT

The objective of our paper is to implement efficient data security (VAPT) Wireless Infrastructure. The wireless infrastructure to be created is seen as complementary to the LAN infrastructure already in place. The objective is also to facilitate mobility and, in particular the information access, exchange and sharing among the users. To ensure interoperability of WLAN (Wireless Local Area Network) products, the wireless fidelity or WiFi Sticker (Wi-Fi Alliance) is also a requisite. In terms of compliance with security and encryption standers, the equipment should support IEEE 802.1x, and be upgradeable to support the standard WPA (wi-Fi protected Access) and WPA2. Sensitive and confidential data are a requisite for most companies, so protection for this data takes great attention by top management of a company, administrators and IT managers. Data leakage cause negative impact on companies. The traditional security approaches, such as firewalls, can't systems are solutions that protect data from leakage, Data leakage/ loss prevention (DLP) non-trusted hands. This paper is an attempt to survey and study DLP systems that will be conducted as well as a comparison with other security and data protection approaches.

Keywords – Data, information technology, professional software and protection

INTRODUCTION

Freedom is the new driving force in telecommunications. With access and speed now consumers want to connect to the wired world without wires. Service providers are, therefore, focused on wireless networking to extend the reach of existing infrastructures. Likewise, enterprises are turning to wireless deployments as a means of facilitating productivity and providing easy access for increasingly mobile workforces. There are a number of technologies commonly referred to as wireless and it important to lay the groundwork for the discussion of the various kinds of wireless.

This technology offers the opportunity to connect to the Internet from any location in the US. Using the same infrastructure that provides satellite TV service, resellers are offering Internet connectivity for home, business and mobile uses. This technology is quite expensive to purchase install and subscribe to. Unless you have no other option for connecting to the Internet,

This wireless technology is most widely used by television remotes. It is also used by Personal Digital Assistants (PDA's) like Palm Pilots to transfer information. Portable printers and other peripheral devices also use it. This technology is very slow and does not offer any great advantages to nonprofits other than some simple conveniences. It has more capabilities than infrared, but still very local "in the room" wireless technology.

DLP (DATA LOSS PREVENTION): Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response [1] Data loss protection is a term that has percolated up from the alphabet soup of computer security concepts in the past few years. Known in the past as information leak detection and prevention (ILDP), used by IDC; information protection and control (IPC); information leak prevention (ILP), coined by Forrester; content monitoring and filtering (CMF), suggested by Gartner; or extrusion prevention system (EPS), the opposite of intrusion prevention system (IPS), the acronym DLP seems to have won out.

Existing technologies used in data prevention: Even before the Internet and all the wonderful benefits it brings to the world, organizations' data were exposed to the outside world. Modems, telex, and fax machines were some of the first enablers of electronic communications. The common thread in these technologies: Keep the "bad guys" out while letting normal, efficient business processes occur. These technologies initially offered some very highlevel, no granular features such as blocking a TCP/IP port, allowing communications to and from a certain range of IP addresses, identifying keywords (without context or much flexibility), signatures of viruses, and blocking spam that used common techniques used by spammers. DLP is like the layers of an onion. Once the first layer of protection is implemented, the next layer should or could be addressed. There are many different forms of DLP applications, depending on the velocity and location of the sensitive data.

Data in Motion: Data in motion is an easy place to start implementing a DLP application because most can function in "passive" mode, meaning it looks at only a copy of the actual data egressing/ ingressing the network.

Data at Rest: Static computer files on drives, removable media or even tape can grow to the millions in large multinational organizations. Unless tight controls are implemented, data can spawn out of control. Even though email transmissions account for more than 80% of DLP violations, data-at-rest files that are resting where they are not supposed to be can be a major concern.

Data in Use: DLP applications can also help keep data where it is supposed to stay. Agent-based technologies that run resident on the guest operating system can track, monitor, block, report, quarantine or notify the usage of particular kinds of data files and/or the contents of the file itself. Policies can be centrally administered and "pushed" out of the organization's computer assets.

Data loss prevention solves three main objectives that are common pain points for many organizations: personal information protection or compliance, intellectual property (IP) protection, and data visibility [2]

IP Protection: Does your organization have important intellectual property and trade or state secrets that could put your organization's financial health and brand image at risk if lost or stolen? DLP solutions like Digital Guardian that use context-based classification can classify intellectual property in both structured and unstructured forms. With policies and controls in place, you can protect against unwanted exfiltration of this data.

Data Visibility: Is your organization seeking to gain additional visibility into data movement? A comprehensive enterprise DLP solution can help you see and track your data on endpoints, networks, and the cloud. This will provide you with visibility into how individual users within your organization interact with data. While these are the three main use cases, DLP can remediate a variety of other pain points including insider threats, Office 365 data security, user and entity behavior analysis, and advanced threats.

DATA LOSS PREVENTION BEST PRACTICES

It is important to determine primary data protection objective. The organization may be trying to protect its intellectual property, gain more visibility into the data, or meet regulatory compliance? With a main objective in place, it's easier to determine the most appropriate DLP deployment architecture or combination of architectures. The four main DLP deployment architectures are: Endpoint DLP, Network DLP, Discovery, and Cloud. DLP is not a security-only decision. It can be implemented according the business needs and size of the budget. Leverage the pain points of different business units to show how DLP can address them. For example, the CFO's pain points include efficient use of assets and profitable growth. Managed DLP services address these pain points by eliminating the need for additional staff and CapEx to When researching DLP vendors, establish your deploy and maintain a DLP program [3]

Pragmatic Data Security Cycle: Figure 1. Clearly define the roles and responsibilities of the individuals involved in your organization's DLP program. Building out role-based rights and duties will provide checks and balances. Start with a clearly defined quick win. Organizations often try complicated initial rollout plans or try to solve too many use cases at once. Define your initial approach and set objectives that are fast and measurable. You should either take the project approach, where you narrow in and focus on a specific data type, or the data visibility approach, where your primary focus is discovery and automated classification of sensitive data to control egress. Work together with business unit heads to define the DLP policies that will govern your organization's data. This will help ensure that the different business units are aware of the policies in place and how they might be impacted (4).

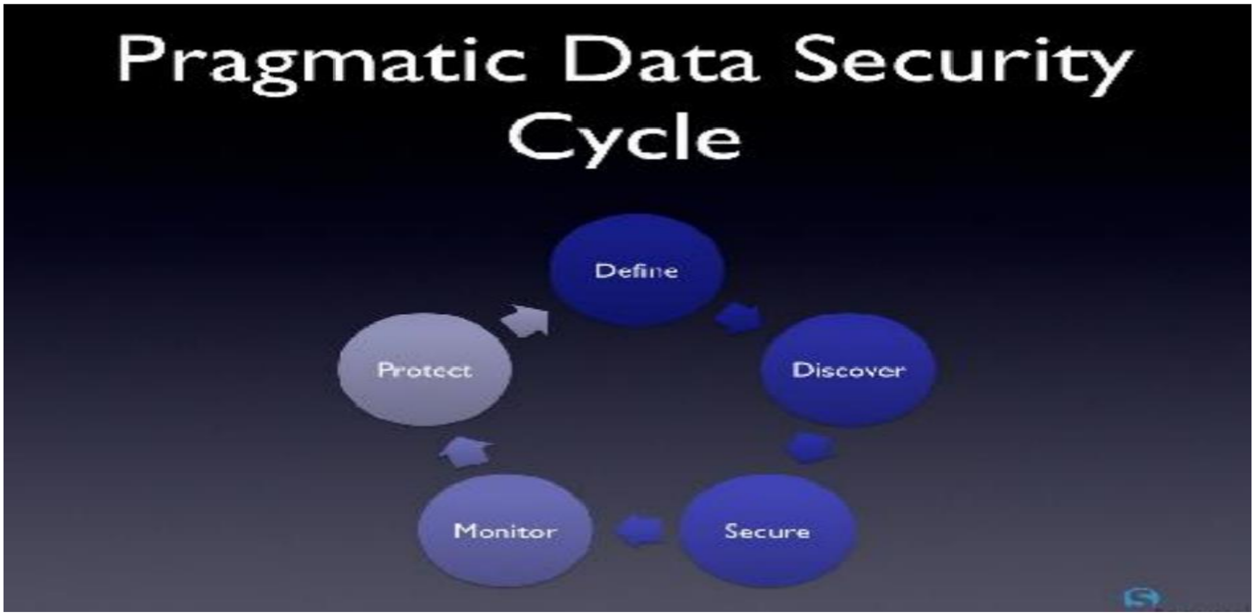

Pragmatic Data Security Cycle

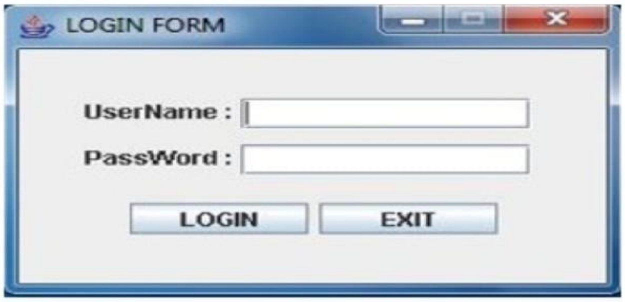
Figure 1. Pragmatic Data Security Cycle

RESULT AND DISCUSSIONS

The User has got Administrative privileges by admin through the admin test case study (Table 1 and Figure 1).

Table 1: Test case study for admin login.

TEST CASE ID	1
Purpose	To login as Admin
Input	Input the admin' s username &password
Expected Result	User should log in as admin
Actual Result	The User has got Administrative privileges by admin



LOGIN FORM

UserName :

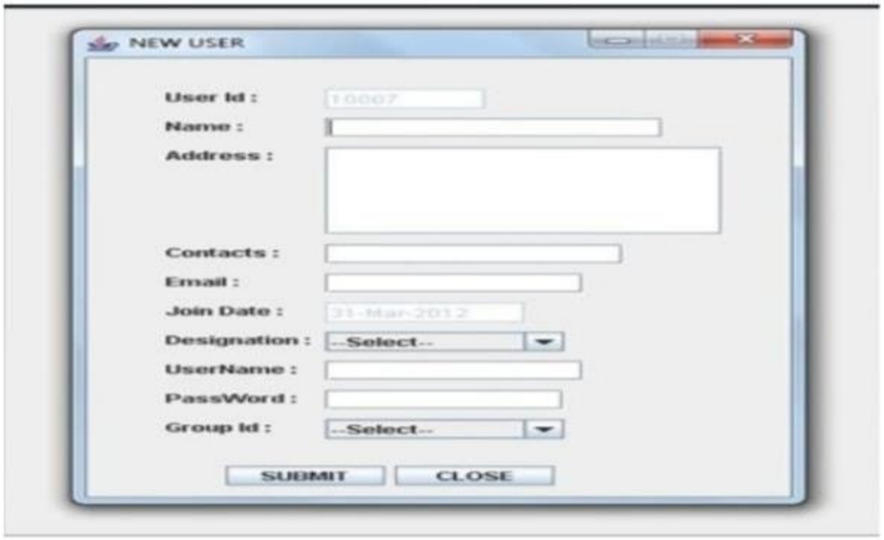
PassWord :

FIGURE 1. Admin login user

A new user is created in the database through the login admin test case study (Table 2 and Figure 2).

Table 2: Test case study for admin login.

TEST CASE ID:	2
Purpose :	To create a user.
Input :	Input a username & his details by logging in admin.
Expected Result:	When submit button is pressed, new user should be created.
Actual Result :	A new user is created in the database.



NEW USER

User Id : 10007

Name :

Address :

Contacts :

Email :

Join Date : 31-Mar-2012

Designation : --Select--

UserName :

PassWord :

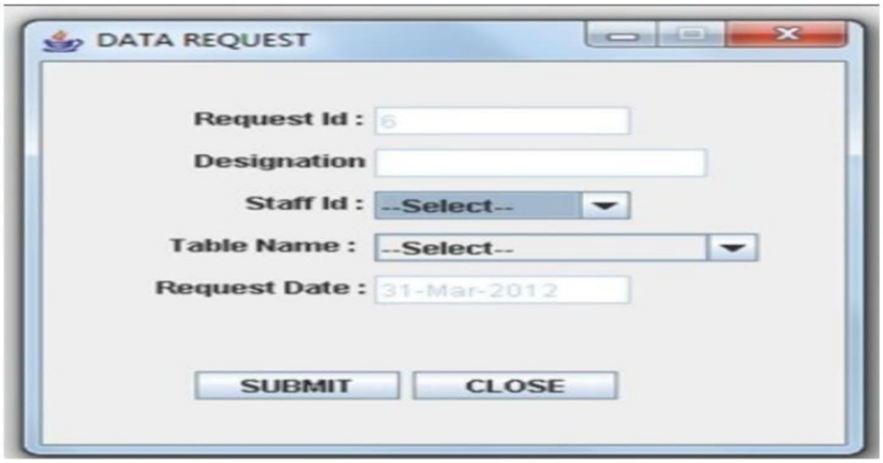
Group Id : --Select--

Figure 2: To create a user

Data sharing and owner of the data can trace the flow of data through input of user request in same group test case study (Table 3 and Figure 3).

Table 3: Data is shared and the owner of the data can trace the flow of data

TEST CASE ID:	3
Purpose :	To allow sharing of data.
Input :	Request a user of the same group for the data.
Expected Result:	If the user accepts the request then the data is shared and the owner of the data can see the flow of the data.
Actual Result :	After accepting the request the data is shared and the owner of the data can trace the flow of data.



Request Id : 6

Designation

Staff Id : --Select--

Table Name : --Select--

Request Date : 31-Mar-2012

FIGURE 3: To allow sharing of data

The owner of the data can see the guilty agent by tracing the flow of data through input of user request in different group test case study (Table 4 and Figure 4-6).

Table 4: The owner of the data can see the guilty agent by tracing the flow of data

TEST CASE ID:	4
Purpose :	To trace data leakage.
Input :	Request a user of different group for unauthorized data sharing.
Expected Result:	Upon acceptance of this unauthorized request, owner of the data can find the agent guilty of data leakage.
Actual Result :	The owner of the data can see the guilty agent by tracing the flow of data.

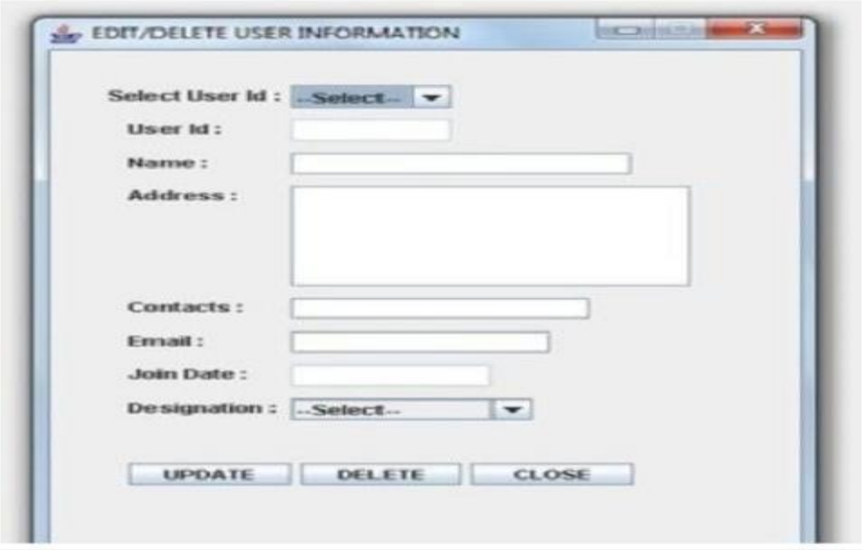
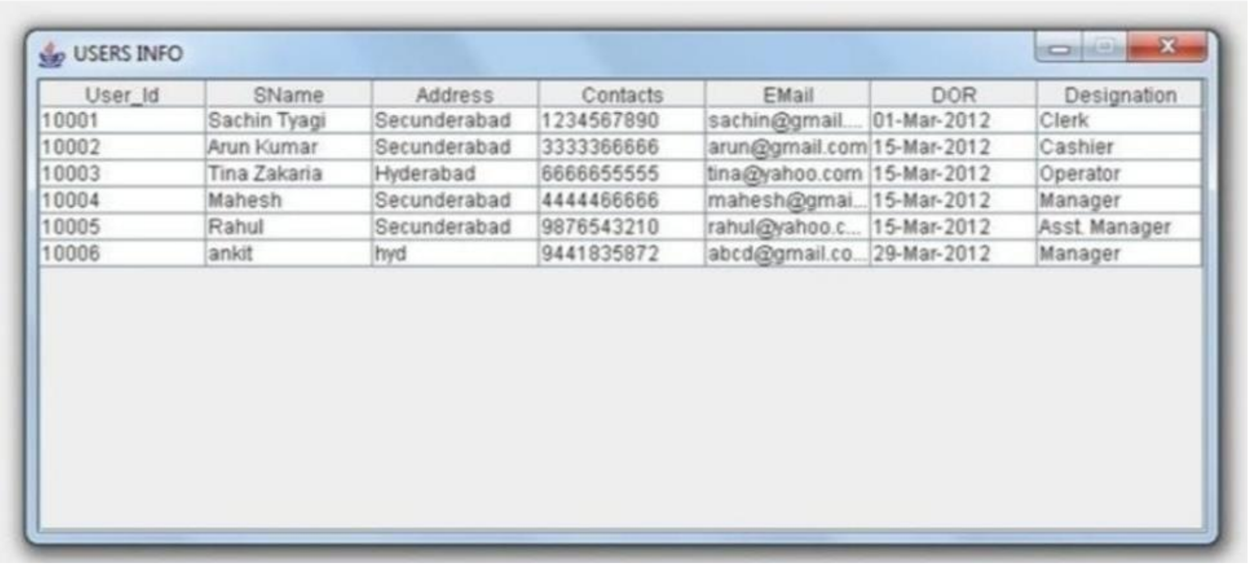
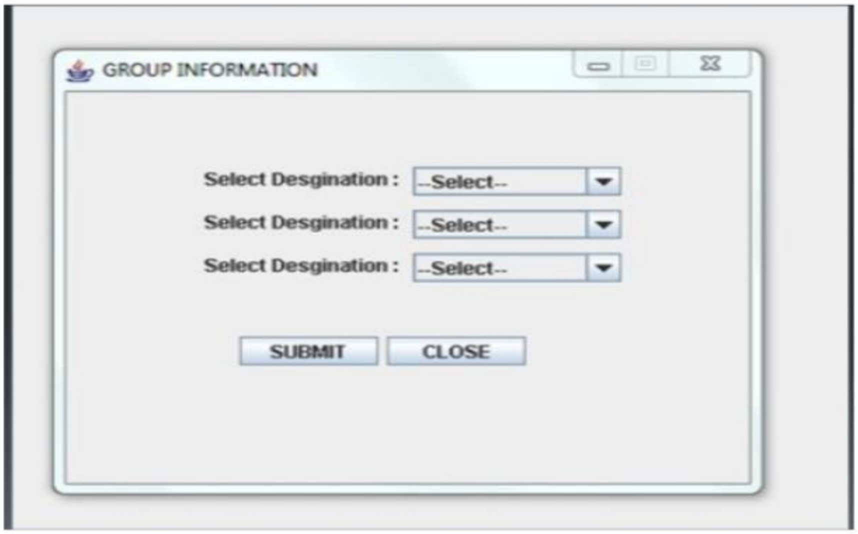


Figure 4: Edit / Delete User Information



User_Id	SName	Address	Contacts	EMail	DOR	Designation
10001	Sachin Tyagi	Secunderabad	1234567890	sachin@gmail....	01-Mar-2012	Clerk
10002	Arun Kumar	Secunderabad	3333366666	arun@gmail.com	15-Mar-2012	Cashier
10003	Tina Zakaria	Hyderabad	6666655555	tina@yahoo.com	15-Mar-2012	Operator
10004	Mahesh	Secunderabad	4444466666	mahesh@gmai...	15-Mar-2012	Manager
10005	Rahul	Secunderabad	9876543210	rahul@yahoo.c...	15-Mar-2012	Asst. Manager
10006	ankit	hyd	9441835872	abcd@gmail.co...	29-Mar-2012	Manager

Figure 5: View user information



Select Desgination : --Select--

Select Desgination : --Select--

Select Desgination : --Select--

Figure 6: Set groups

802.11 standard supports Wireless Equivalent Privacy (WEP)-based security. WEP security allows all data communication between wireless LAN clients and/or APs in encrypted form. Use the settings on this tab to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall (5).

At the end of the day the DLP market and applications are maturing at an incredible pace. Vendors are releasing new features and functions almost every calendar quarter. In the past, when monitoring seems sufficient to diagnose the central issue of data security, the marketplace was demanding more control, more granularity, easier user interfaces, and more actionable reports, as well as moving the DLP application off the main network egress point and parlaying the same functionality to the desktop/laptops, servers, and their respective end points to document storage repositories and databases. In evaluating DLP applications, it is important to focus on the type of underlying engine that analyzes the data and then work up from that base. Next rate the ease of configuring the data categories and the ability to preload certain documents and document types. Look for a mature product with plenty of industry-specific references.

Company stability and financial health should also come into play. Roadmaps of future offerings can give an idea of the features and functions coming in the next release. The relationship with the vendor is an important requirement to make sure that the purchase and subsequent implementation goes smoothly. The vendor should offer training that empowers the IT organization to be somewhat self-sustaining instead of having to go back to the vendor every time a configuration needs to be implemented. The vendor should offer best practices that other customers have used to help with quick adoption of policies. This allows for an effective system that will improve and lower the overall risk profile of the organization. Analyst briefings about the DLP space can be found on the Internet for free and can provide an unbiased view from a third party of things that should be evaluated during the selection process [6-7].

In addition to securing against outside threats, preventing data loss is an essential component of data security. Data and crosswalks between study IDs and PII should be backed up regularly in at least two separate locations, and passwords must not be forgotten.

SUMMARY AND CONCLUSION

DLP is an important tool that should at least be evaluated by organizations that are looking to protect their employees, customers, and stakeholders. An effectively implemented DLP application can augment current security safeguards. A well thought out strategy for a DLP application and implementation should be designed first before a purchase. All parts of the organization are likely to be impacted by DLP, and IT should not be the only organization to evaluate and create policies. A holistic approach will help foster a successful implementation that is supported by the DLP.

Vendor and other departments, and ultimately the employees should improve the data risk profile of an organization. The main goal is to keep the brand name and reputation of the organization safe and to continue to operate with minimal data security interruptions. Many types of DLP approaches are available in the market today; picking the right vendor and product with the right features and functions can foster best practices, augment already implemented employee training and policies, and ultimately safeguard the most critical data assets of the organization.

REFERENCES

1. Tahboub R Saleh Y. Data Leakage/Loss Prevention Systems (DLP). 2014 World Congress on Computer Applications and Information Systems (WCCAIS) Publisher: IEEE 2014 pp: 1-6.
2. Tomoyoshi Hiroshi T Takayuki T Ryusuke Masuoka H. Fujitsu. Data Loss Prevention Technologies. Sci. Tech. J. 2010 vol: 46 (1) pp: 47-55.
3. Berlee, Anna. 2015. "Using NYC Taxi Data to identify Muslim taxi drivers." The Interdisciplinary Internet Institute (blog). Accessed November 30, 2015. http://theiii.org/index.php/997/using-nyc-taxi-data-to-identifymuslim-taxi-drivers/.
4. Goodin, Dan. 2014. "Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts." Ars Technica. Accessed November 30, 2015. http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logsreveal-nyc-cab-drivers-detailed-whereabouts.
5. Mangan, Katherine. 2010. "Chapel Hill Researcher Fights Demotion after Security Breach." Chronicle of Higher Education. Accessed March 7, 2018. https://www.chronicle.com/article/chapel-hill-researcherfights/124821/.
6. Narayanan, Arvind, and Vitaly Shmatikov. 2008. "Robust De-Anonymization of Large Sparse Datasets." presented at the Proceedings of 29th IEEE Symposium on Security and Privacy, Oakland, CA, May. http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf/.
7. Pandurangan, Vijay. 2014. "On Taxis and Rainbows: Lessons from NYC's improperly anonymized taxi logs." Medium. Accessed November 30, 2015. https://medium.com/@vijayp/of-taxis-and-rainbows.