“SAN FRANCISCO POLICE DEPARTMENT ENCRYPTING THEIR COMMERCIAL AGENCY COMMUNICATIONS”

Sreekar Bathula

Id: 28067764

Master’s in business analytics

Hult international business school

Content

1. Summary

SFPD (“San Francisco Police Department”), the second largest police force in “California, USA,” appears to be the largest police force in the state, reporting 2,100 employees and encrypting all wireless traffic in December. . SFPD began encrypting all wireless communications and making them inaccessible to the public in order to avoid surveillance of local police channels and threats to public safety. Working with the California Department of Justice, the SPFD also tends to protect personally identifiable information (PII). For removing barriers to police accountability and advocating for the community as a meaningful privacy protection.

2. Ethical dilemma

Reportedly, numerous police scanners, hobbyists, and technicians routinely intercept police activity. Communications between the SFPD and the city's Emergency Management Agency (DEM) have been heard before. Emergency calls from the police and fire department were also played on the radio in advance. Even standard police maneuvers could be heard from the police stream. Privacy law experts believe comprehensive encryption is an extreme response to a publicly perceived threat, radio is a necessary public response, and police radio transmissions a necessary public resource. That's why it says it's encrypted. By restricting the transmission of personally identifiable information, authorities encoded some of the radio traffic with sensitive information, such as discussions of sexual assault and domestic violence. Scanner aficionados on radio forums and subreddits were the first to notice the change, with many saying it could undermine police transparency at a time of heightened mistrust of the police. was concerned. You tracked the division's move from an analog radio system to a digital radio system in November. SFPD has replaced the 20-year-old system with a new version that provides wider coverage, clearer audio and complies with interoperability standards.

3. Solution

Sensitive information must be encrypted to keep the police system transparent and accountable. Communications with SFPDs, PII, and DEMs should be encrypted and restricted to the public. This is a cyber attack he should not affect SFPD and the general public. Quick access to information saves lives. Making that content relevant, factual, and

easily accessible is at the core of our mission. In order to maintain transparency of information, SFPD should keep the necessary information open. It poses a far greater obstacle to police accountability and community defense than to meaningful privacy protection.

Regarding public protection and public data confidentiality, SFPD should continue to improve the system, update everything, encrypt and publish. Publish only necessary information.

If you need this kind of program, please consider legal and administrative cyber security and create a new version.

4. My opinion

My strict opinion is in favor of SFPD encrypting the radio transmission, and communication with PII and DEM.

Reasons to support

4.1 Improving data security: Store, manage, or transmit sensitive data - You must allow us to use best available techniques to thwart attacks on that data or on businesses and individuals.

4.2 Enhancing law enforcement and counter-terrorism capabilities: Law enforcement agencies must have access to the best available resources, information and tools to prevent and prosecute terrorist and criminal acts, provided they adequately protect privacy and civil liberties.

4.3 Promoting privacy: Individuals have the right to security in their public, private and business lives and interactions..

4.4 Protecting confidential government information: National, state, and local governments must ensure that the data they hold is protected from threats from domestic and foreign intruders.

4.5 Encouraging innovation: Developers and providers of innovative data security tools should be freed from government contracts to design digital security technology products and tools.

4.6 Defending critical infrastructure: Providers of critical services such as banks, healthcare, electricity, water, and other critical infrastructure providers need to be able to provide their users with the best security technology available. Best practices should be widely disseminated.

4.7 Understanding the global impact: Criminal and terrorist acts are not restricted by national borders. Laws and policies must provide consistency and clarity in all countries where security technologies are developed and deployed.

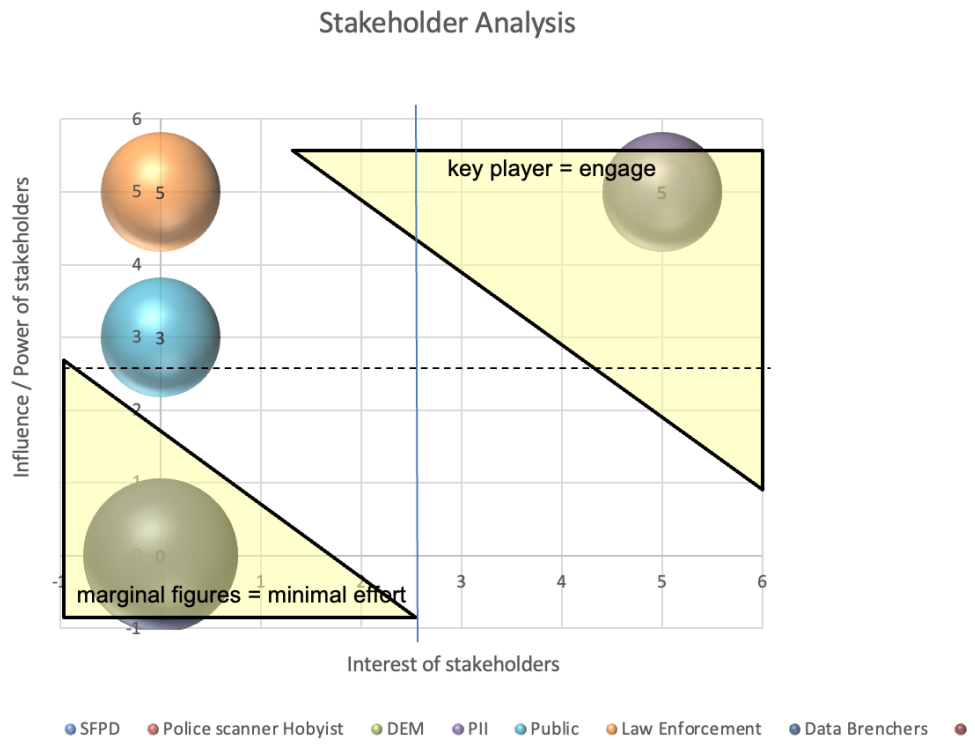
4.8 Increasing transparency: We need a full, transparent, and considered public dialogue before adopting any legislative proposal on technology procurement or the future of cryptography.

5. Stakeholder analysis - 1

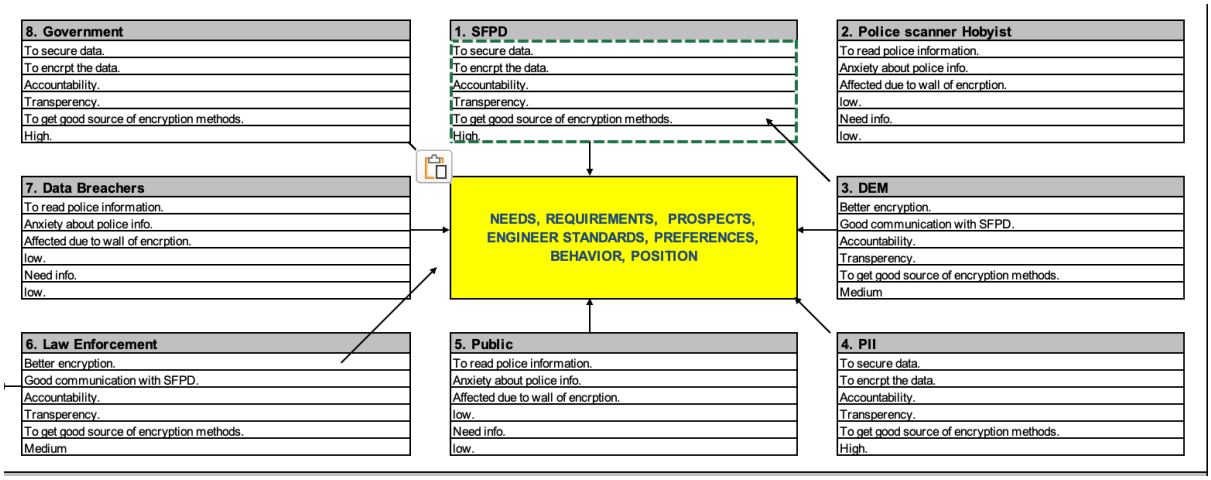
Student Name:	
Sreekar Bathula	**Stakeholder Analysis 1**

"The stakeholder analysis is an instrument to illustrate and to discover different needs of different stakeholders of particular companies"

	Stakeholder	Interest of stakeholders	Influence/Power of stakeholders	Preferences (possitive / negative)
		[0;5] - [0=small; 5=big]	*[0;5] - [0=small; 5=big]*	*[1;3;5] - [1=pos; 3=neutral; 5=neg]*
1.	SFPD	5	5	1
2.	Police scanner Hobyist	0	0	5
3.	DEM	5	5	3
4.	PII	5	5	3
5.	Public	0	3	3
6.	Law Enforcement	0	5	3
7.	Data Brenchers	0	0	5
8.	Government	5	5	1



6. Stakeholder analysis - 2



Step 1: Evaluation of Stakeholders

Who can/could exert influence? – SFPD.

Who has legitimate claims? – Police scanner hobbyist.

Step_2: Classification of Stakeholders

Amount of influence and suggestibility – Law enforcement.

Concernment – SFPD, Public

Step_3: Assessment of Claims

Expectations of harm/good? – SFPD, Public.

Legitimacy and reasonability? – Government.

Step_4: Activities

inform, involve, bargain – SFPD to Government to Law enforcement to Public.

open and close – SFPD and Government.

7. Reference list

https://www.buzzfeednews.com/article/sarahemerson/sfpd-has-blocked-public-from-most-radio-broadcasts

https://epic.org/buzzfeed-the-san-francisco-police-department-has-encrypted-its-radio-feeds/

https://encryption.bsa.org/

Hamilton, G., 2021. Facial Recognition Regulations: A Review of The Current Legal Restrictions Imposed on The Technology's Use in the United States (Doctoral dissertation, Villanova University).

Waghorne, S., 2022. The Price of Privacy: a Call for a Blanket Ban on Facial Recognition in the City of St. Louis. Washington University Journal of Law and Policy, 69(1).

Fleischer, R.S., 2020. Bias In, Bias Out: Why Legislation Placing Requirements on the Procurement of Commercialized Facial Recognition Technology Must Be Passed to Protect People of Color. Public Contract Law Journal, 50(1), pp.63-89.

Bigos, M.A., 2021. Let's" Face" It: Facial Recognition Technology, Police Surveillance, and the Constitution. J. High Tech. L., 22, p.52.

Chilson, N.A. and Barkley, T.D., 2021. The Two Faces of Facial Recognition Technology. IEEE Technology and Society Magazine, 40(4), pp.87-100.

Franco-Trigo, L., Fernandez-Llimos, F., Martínez-Martínez, F., Benrimoj, S.I. and Sabater-Hernández, D., 2020. Stakeholder analysis in health innovation planning processes: a systematic scoping review. Health Policy, 124(10), pp.1083-1099.