Using Facial Recognition to gather Social Media Intelligence

Jack Neilson

January 22, 2018

1 Literature Review

1.1 Background

1.1.1 SOCMINT

Social media intelligence (SOCMINT) is an emergent field in intelligence gathering where data is gathered from social media profiles. Massive amounts of data are added to social media services every day (Omand et al., 2012), much of it personal, making social media sites a potentially valuable resource when gathering information about groups or individuals (Ruiz, 2018). Social networks have also been used as a means of communication between persons of interest to the security services, making mining intelligence from their profiles a high priority (Omand et al., 2012)(Kilburn and Krieger, 2014)(Unknown, 2013).

As it stands, social media intelligence sources are woefully underutilised. After the 2011 riots in London that were organised in large part on social media, Her Majesty's Inspectorate of Constabulary stated that the police services were ”insufficiently equipped” to effectively use SOCMINT in their response(Antonius and Rich, 2013). This is not to say that the value of SOCMINT is not realised however, as many intelligence agencies are investing in tools to effectively gather and analyse SOCMINT (Antonius and Rich, 2013) or are performing case studies in to potential uses (Klontz and Jain, 2013).

1.1.2 Uses of SOCMINT

1.1.3 Current Applications

1.1.4 Facial Recognition

1.1.5 Uses of Facial Recognition

1.1.6 Constrained vs Unconstrained

1.2 Theory

1.2.1 Prior Work

1.2.2 Individual vs Group Data

1.2.3 Quantity of Information

1.2.4 Accessibility of Data

1.2.5 Uses

1.2.6 Challenges and Constraints

1.3 SOCMINT

1.3.1 Prior Knowledge Attacks

1.3.2 HUMINT

1.3.3 Social Engineering

1.3.4 Spearphish

1.4 Facial Recognition

Overview and current applications

1.4.1 Challenges

1.4.2 Recent Advances

1.4.3 Unconstrained Facial Recognition

References

Antonius, N. and Rich, L. (2013), ‘Discovering collection and analysis techniques for social media to improve public safety’, **3**, 42.

Kilburn, M. and Krieger, L. (2014), ‘Policing in an information age: The prevalence of state and local law enforcement agencies utilising the world wide web to connect with the community’, *International Journal of Police Science & Management* **16**(3), 221–227.
URL: *https://doi.org/10.1350/ijps.2014.16.3.341*

Klontz, J. C. and Jain, A. K. (2013), ‘A case study on unconstrained facial recognition using the boston marathon bombings suspects’, *Michigan State University, Tech. Rep* **119**(120), 1.

Omand, S. D., Bartlett, J. and Miller, C. (2012), ‘Introducing social media intelligence (socmint)’, *Intelligence and National Security* **27**(6), 801–823.
URL: *https://doi.org/10.1080/02684527.2012.716965*

Ruiz, J. (2018), Gchq and mass surveillance, Technical report, Open Rights Group.

Unknown (2013), ‘Prism slides’, Leaked to several newspapers by Edward Snowden in late 2013.