Weaving a Safe Web of News

Kanak Biscuitwala[*]
kanak@cs.stanford.edu

Willem Bult[*]
wbult@stanford.edu

Mathias Lécuyer[†]
ml3302@columbia.edu

T.J. Purtell[*]
tpurtell@cs.stanford.edu

Madeline K.B. Ross[‡]
mkr2132@columbia.edu

Augustin Chaintreau[†]
augustin@cs.columbia.edu

Chris Haseman[§]
haseman@tumblr.com

Monica S. Lam[*]
lam@cs.stanford.edu

Susan E. McGregor[‡]
sem2196@columbia.edu

[*]Computer Science Department, Stanford University
[†]Computer Science Department, Columbia University
[‡]Graduate School of Journalism, Columbia University
[§]Tumblr, Inc.

> "Skype has gone from in the mid-2000s being the tool most widely used and promoted by human rights activists to now when people ask me I say, 'Definitely, don't use it,' "
>
> – Ronald J. Deibert, cited in *New York Times*[1], November 30, 2012

1. INTRODUCTION

The rise of social media and data-capable mobile devices in recent years has transformed the face of global journalism, supplanting the broadcast news anchor with a new source for breaking news: the citizen reporter. Social media's decentralized networks and instant re-broadcasting mechanisms mean that the reach of a single tweet can easily trump that of the most powerful broadcast satellite. Brief, text-based and easy to translate, social messages allow news audiences to skip the middleman and get news "straight from the source."

Whether used by "citizen" or professional reporters, however, social media technologies can also pose risks that endanger these individuals and, by extension, the press as a whole. First, social media platforms are usually proprietary, leaving users' data and activities on the system open to scrutiny by collaborating companies and/or governments. Second, the networks upon which social media reporting relies are inherently fragile, consisting of easily targeted devices and relatively centralized message-routing systems that authorities may block or simply shut down. Finally, this same privileged access can be used to flood the network with inaccurate or discrediting messages, drowning the signal of real events in misleading noise.

A citizen journalist can be anyone who is simply **in the right place at the right time**. Typically untrained and unevenly tech-savvy, citizen reporters are unaccustomed to thinking of their social media activities as high-risk, and may not consider the need to defend themselves against potential threats. Though often part of a crowd, they may have no formal affiliations; if targeted for retaliation, they may have nowhere to turn for help. **The dangers citizen journalists face are personal and physical**. They may be targeted in the act of reporting, and/or online through the tracking of their digital communications. Addressing their needs for protection, resilience, and recognition requires a move away from the major assumptions of *in vitro* communication security. For citizen journalists using social networks, *the adversary is already inside*, as the network itself may be controlled or influenced by the threatening party, while "outside" nodes, such as public figures, protest organizers, and other journalists can be trusted to handle content appropriately. In these circumstances there can be no seamless, guaranteed solution. Yet the need remains for technologies that improve the security of these journalists who in many cases may constitute a region's only independent press.

In this paper, we argue that a comprehensive and collaborative effort is required to make *publishing* and *interacting* with news websites more secure. Journalists typically enjoy stronger legal protection at least in some countries, such as the United States. However, this protection may prove ineffective, as many online tools compromise source protection. In the remaining sections, we identify a set of discussion topics and challenges to encourage a broader research agenda aiming to address jointly the need for social features and security for citizens journalists and readers alike. We believe communication technologies should embrace the methods and possibilities of social news rather than treating this as a pure security problem. We briefly touch upon a related initiative, *Dispatch*, that focuses on providing security to citizen journalists for publisihing content.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design; J.7 [**Computer Applications**]: Computers in Other Systems—*publishing*

Keywords

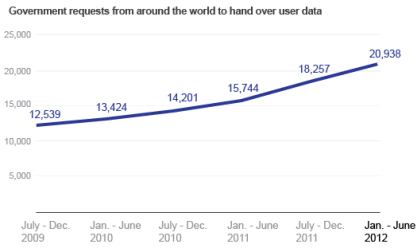
Mobile publishing; Disconnection resilience

2. THE WEB OF NEWS UNDER THREAT

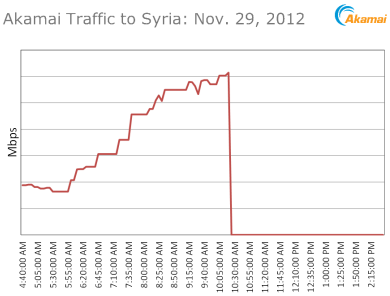
The current digital communication landscape is characterized by enormous potential and innumerable threats. Thanks to social media's substantial role in publicizing the events of the Arab Spring, the eventual overthrow of Egypt's government in 2011 was often referred to as the "Facebook and Twitter revolution"[21], with pictures of protesters

[1]In "For Syria's Rebel Movement, Skype Is a Useful and Increasingly Dangerous Tool", by A. Chozick

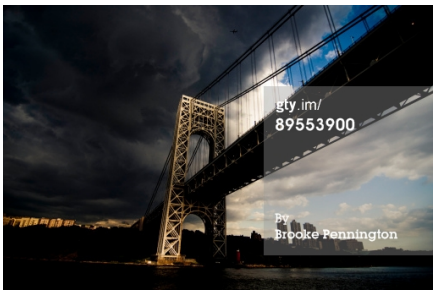
WWW 2013 Companion, May 13–17, 2013, Rio de Janeiro, Brazil.
ACM 978-1-4503-2038-2/13/05.



TM-1



TM-2



TM-3

Figure 1: Threats to citizen journalists, illustrated with three recent examples. (TM-1) Surveillance: rise of government access to data stored on online media companies, self-reported by Google on November 13th, (TM-2) Disconnection: Internet black-out in Syria, as reported by Akamai on November 29th, (TM-3) Discredit: a 2009 Getty Stock picture, viral during Sandy, later identified as a fake report.

thanking social media companies highly publicized even by traditional media outlets. Although the exact role of social media in the revolution itself is subject to debate [11, 22, 28], its importance was credited by participants[2], and they were instrumental in increasing awareness and worldwide engagement [1]. What we will never know is how many individuals were tracked, targeted or discredited through these same social media channels.

We do know, however, that even in the U.S. content contributors are at risk of being physically tracked through their digital communications[3]. This is to say nothing of regimes where individuals may find their content filtered or blocked, or their reputation manipulated. These vulnerabilities are artifacts of the current architecture of networked communication and publishing platforms, including social media:

1. Even in countries with strong privacy laws, the data hosted and published by service providers on users' behalf is often exempt from protection. It is common for governments to ask companies like Google to turn over user data, and in many places - including the U.S. - the current legal framework requires full compliance[4]. In other cases, regimes can use network surveillance technologies to monitor traffic directly[5].

2. Access to publishing platforms and social media can be easily disrupted by blacklisting circumvention tools like Tor and blocking access to certain servers. As seen in Egypt and Syria, regimes can choose in extreme cases to "go dark," blocking all Internet traffic to the outside world. Even in the United States, targeted censorship of this style has been executed over small areas through strategic deployment of signal jammers[6].

3. Influential entities can employ structured campaigns to discredit or bury unwanted messages, or even prevent initial publishing through threats or direct attacks. The power relationship between citizen journalists and corporate or government actors is highly asymmetric. Citizen journalists are unpaid, operating alone or in only loose coordination with others, while corporations and governments are organized and often well-funded. Averting these attacks requires messaging to be both anonymous *and* authenticated.

[2]"When I asked the Islamist Jlassi why the revolution had not happened a decade earlier in Tunisia, he instantly answered, 'Al-Jazeera and the Internet were the differences, especially Al-Jazeera - everybody watches TV.'" in *Time*, December 14, 2011

[3]See T. Kary, "Twitter Turns Over Wall Street Protester Posts Under Seal", *Bloomberg*, September 14, 2012

[4]See D. Chou, "Transparency Report: Government requests on the rise", *Google Official Blog*, November 13, 2012.

[5]See S. Stecklow, "Special Report: How foreign firms tried to sell spy gear to Iran", *Reuters*, December 5, 2012

[6]See M. Bell, "BART San Francisco cut cell services to avert protest" *Washington Post*, August 12, 2011

Threat Model.

We identify three Threat Models (TM) that few, if any, current solutions fully address (See recent examples in Figure 1): **TM-1: Detect and Detain**. In this model the adversary is seeking not disruption but information, by observing journalists' communication or requesting their data. While certain kinds of data interception are not legal, the same ends can often be achieved through legal means (such as subpoena), or simply by participating in the network directly. In all cases, adversaries can usually gather users' personal information, and even physically track their movements. **TM-2: Filter and Disconnect**. Here, the adversary is active and attempts to censor digital communication. While blocking transmissions to foreign servers or taking down the network entirely is feasible, it is costly and highly profile. A more common - and insidious - approach, then, it is to maintain some services, such as e-commerce, while censoring undesirable messages. **TM-3: Pollute and Manipulate**. In this last model, the adversary may flood the system with irrelevant or inaccurate information, either to overwhelm the transmission of legitimate messages, or to transmit a biased view of a situation. Alternatively, the adversary may pose as a citizen reporter and execute targeted attempts to discredit or defame a particular journalist.

3. CHALLENGES

Assessing the Publishing Needs of Citizen Journalists.

In theory, professional journalists can rely on their affiliated organization to provide them with some safety training and legal support. Realistically, newsrooms' technical expertise is often limited, and cash-strapped organizations must

rely more on freelancers of varying experience levels. **As so much of today's essential journalism is being executed by citizen reporters, better protections from the current vulnerabilities of networked publishing platforms like social media are essential to preserving and promoting journalism worldwide**. We believe these vulnerabilities can be credibly addressed and we identify at least three related areas of research:

1. Creating and maintaining a pseudo-anonymous presence that remains *isolated* from a physical identity. While this is a classic computer security problem, it remains a significant issue for users of platforms like Twitter and Facebook, which require users to maintain a single identity, often connected to personally identifiable data. Combined with proprietary mobile operating systems, it becomes easier every day for third parties to connect user data not just across the web, but to connect these activities to actual, physical devices [24, 8, 17]. Even the incomplete data about an individual obtained through social media can yield accurate details about that person's physical identity, even if it is meant to be private and secret [20, 26, 18, 19].

   The most immediate challenge in this area is support the use of encryption schemes by improving their usability. Also, indirect information leaks should be insured against use as an attack vector against users.

2. Building social media applications that are *resilient* to censorship and disconnection. Recent works [3, 9, 25], including ours [23, 6], proved that one can deliver content between mobile phones efficiently with minimum or even nonexistent network support. Unfortunately, most of these protocols have either not been tested in practice [13], or only within a friendly environment of cooperative nodes [4].

3. Developing systems to harness the power of the crowd and social networks to handle pollution and manipulation. Systems that protect identities are always vulnerable to pollution attacks through content injection and fake identities [7]. However, it has repeatedly been shown that properties of large systems can be used to detect manipulation [30, 29, 27].

   Through a combination of rate limiting and offline certification among trusted members, a system's tolerance for pollution can be reduced. The power of the crowd also can be used to moderate and verify user-generated content [12], as can the application of new distributed algorithms that leverage social properties [14, 15].

Building Tools for News Browsing.

In addition to mechanisms protecting citizen journalists as they *produce* source content for reporters, we believe that more work is needed to protect citizens as they *browse* and *interact* with news websites. Passive news consumption has now been replaced by active commenting on and sharing of news on digital platforms, often mediated by social media. These behaviors can generate risks for users, especially when third parties are involved and/or content is accessed from conflict regions. We identify the following opportunities:

1. Encourage news websites to provide a "safe browsing" mode that protects against third-party monitoring, including that which could be disguised as advertising. These organizations could even help protect against content manipulation by leveraging a network of proxies. This can be facilitated through the reuse of recent work on anonymous and censorship resistant browsing.

2. Allow users to protect their identities and control their data whenever they post comments or share stories online.Through platform-specific trust relationships, users can provide meaningful endorsements or comments without disclosing de-anonymizing information.

3. Offer a service that would monitor users' risk of de-anonymization and inform them of identifying inferences that are possible based on the information they've shared. This would empower users to contribute news websites without fear of compromising their privacy.

4. Provide a system that is censorship tolerant using techniques like [10], to preventing filtering, and blocking of content. Likewise, Content-Centric Networking [2] techniques that rely on user caching (while preserving privacy [16]) could offer data resilience in the case of legal filtering or denial of service attacks.

4. DISPATCH: SAFE PUBLISHING

To encourage further research, we provide an example taken from our recent research: the *Dispatch* project[7] already has an alpha iOS version that was used by journalism students reporting during U.S. election night in New York.

Dispatch offers a tool for citizen reporters to communicate and publish using authenticated pseudonyms. Using identity-based encryption [5], Dispatch messages are directly encrypted and authenticated by those pseudonyms, providing protection against data manipulation and interception. A citizen reporter with this app is able to publish text and images instantly to a blog or a private server if desired; the pseudonym functions seamlessly across multiple social media platforms. Dispatch's routing system addresses messages solely based on hashed recipient pseudonyms, allowing its routing mechanism to be distributed. Leveraging identity-based routing, Dispatch features a disconnected mode that leverages wireless links between users to replicate information and combat service-disruption based censorship. Dispatch is easy to deploy wherever secure communication between sources and journalists is needed. Field tests and presentations of the platform at leading journalism conferences have indicated strong demand for this type of secure, networked publishing and communication tools in the journalism community.

5. ACKNOWLEDGEMENTS

Dispatch is one of the inaugural recipients of a "Magic Grant" from the Brown Institute of Media Innovation. Our research is also supported in part by NSF Programmable Open Mobile Internet (POMI) 2020 Expedition Grant 0832820 and the Stanford MobiSocial Computing Laboratory.

[7]see `http://dispatchapp.wpengine.com`

6. REFERENCES

[1] S. Aday, H. Farell, M. Lynch, J. Sides, and D. Freelon. Blogs and Bullet II: New Media and Conflict After the Arab Spring. *Report to the United States Institute of Peace*, 2012.

[2] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker. On preserving privacy in content-oriented networks. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking*, ICN '11, 2011.

[3] A. Balasubramanian, B. N. Levine, and A. Venkataramani. DTN routing as a resource allocation problem. In *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, 2007.

[4] N. Banerjee, M. Corner, D. Towsley, and B. N. Levine. Relays, base stations, and meshes: enhancing mobile networks with infrastructure. *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008.

[5] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO 2001*, 2001.

[6] A. Chaintreau, A. Mtibaa, L. Massoulié, and C. Diot. The diameter of opportunistic mobile networks. In *CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference*, 2007.

[7] J. Douceur. The sybil attack. *Peer-to-peer Systems*, 2002.

[8] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. TaintDroid: An Information-Flow Tracking System for Realtime PrivacyMonitoring on Smartphones. *In Proceedings of OSDI*, 2010.

[9] K. Fall. A delay-tolerant network architecture for challenged internets. *Proceedings of the 2003 conference on Applications*, 2003.

[10] D. Fifield, N. Hardison, J. Ellithorpe, E. Stark, R. Dingledine, P. Porras, and D. Boneh. Evading Censorship with Browser-Based Proxies. In *Privacy Enhancing Technologies Symposium*, pages 239–258, Vigo, Spain, 2012. Springer.

[11] L. Gawhry. *Assessing the Impact of Social Media on the 25 January 2011 Egyptian Revolution.* Naval Postgraduate school M.A. thesis.

[12] A. Ghosh and P. McAfee. Incentivizing high-quality user-generated content. In *WWW '11: Proceedings of the 20th international conference on World wide web*, 2011.

[13] D. Gunawardena, T. Karagiannis, A. Proutiere, E. Santos-Neto, and M. Vojnovic. Scoop: decentralized and opportunistic multicasting of information streams. In *MobiCom '11: Proceedings of the 17th annual international conference on Mobile computing and networking*, 2011.

[14] S. Ioannidis, A. Chaintreau, and L. Massoulié. Optimal and Scalable Distribution of Content Updates over a Mobile Social Network. *INFOCOM 2009, IEEE*, 2009.

[15] S. Isaacman, S. Ioannidis, A. Chaintreau, and M. Martonosi. Distributed rating prediction in user generated content streams. In *RecSys '11: Proceedings of the fifth ACM conference on Recommender systems*, 2011.

[16] T. Lauinger, T. Strufe, T. UniversitŁt, N. Laoutaris, E. Biersack, P. Rodriguez, and E. Kirda. Privacy implications of ubiquitous caching in named data networking architectures. Technical Report TR-iSecLab-0812-001, iSecLab, 2012.

[17] J. R. Mayer and J. C. Mitchell. Third-Party Web Tracking: Policy and Technology. *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012.

[18] B. Meeder, B. Karrer, A. Sayedi, R. Ravi, C. Borgs, and J. Chayes. We know who you followed last summer: inferring social link creation times in twitter. In *WWW '11: Proceedings of the 20th international conference on World wide web*, 2011.

[19] A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel. You are who you know: inferring user profiles in online social networks. *Proceedings of the third ACM international conference on Web search and data mining*, 2010.

[20] A. Narayanan and V. Shmatikov. De-anonymizing Social Networks. *Security and Privacy, 2009 30th IEEE Symposium on*, 2009.

[21] J. Pollock. Streetbook. *MIT Technology Review*, 2011.

[22] J. Pollock. People Power 2.0. *MIT Technology Review*, 2012.

[23] J. Reich and A. Chaintreau. The age of impatience: optimal replication schemes for opportunistic networks. In *CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies*, 2009.

[24] F. Roesner, T. Kohno, and D. Wetherall. Detecting and defending against third-party tracking on the web. In *NSDI'12: Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, 2012.

[25] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav. Low-cost communication for rural internet kiosks using mechanical backhaul. In *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*, 2006.

[26] M. Srivatsa and M. Hicks. Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel. *CCS '12: Proceedings of the 19th ACM conference on Computer and communications security*, 2012.

[27] B. Viswanath, A. Post, K. Gummadi, and A. Mislove. An analysis of social network-based Sybil defenses. *SIGCOMM '10: Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM*, 2010.

[28] J. C. York. Beyond Streetbook. *MIT Technology Review*, 2012.

[29] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao. SybilLimit: A near-optimal social network defense against sybil attacks. *IEEE/ACM Transactions on Networking (ToN)*, 18:885–898, 2010.

[30] H. Yu, M. Kaminsky, and P. Gibbons. SybilGuard: Defending against sybil attacks via social networks. *IEEE/ACM Transactions on Networking*, 2008.