Digital Security for Trans* Communities

Norman Shamas
Independent Researcher
https://orcid.org/0000-0001-5395-7728
norman.shamas@gmail.com

Co-authored by anonymous trans* activists

ABSTRACT

Despite the examination of digital rights and privacy for marginalised communities within the human rights field and funding, trans* stories and needs are often marginalised and ignored. This article explores the lived realities of US-based trans* communities online. Two example cases are used to demonstrate how the current rhetoric around digital security and privacy does not take into account trans* perspectives. The article ends with some recommendations to improve the field of digital security and conversations on the intersection of trans* communities and digital rights.

Keywords: digital security; trans* communities; identity; lived reality; privacy

Introduction

This article will focus on reality—the reality that trans* communities in the US face every day regarding their identities. This is not about possible threats from nation states or how to protect against a surveillance state that more often targets marginalised communities; it is about lived realities. Due to constraints, this discussion does not include all realities or situations that trans* communities face.[1] Most importantly, this is meant as a starting point. There aren't easy answers and, sometimes, the questions haven't even been asked.

[1] By nature of my experiences, I am talking primarily about trans* communities in the US. The term "trans*" in and of itself is complicated and problematic, especially when talking about global communities that had unique identities prior to the categorisation of specific people as "trans*."

Gender Questions
https://upjournals.co.za/index.php/GQ/index
Volume 5 | Number 1 | 2017 | #4120 | 7 pages

https://doi.org/10.25159/2412-8457/4120
ISSN 2412-8457 (Online), ISSN 2309-9704 (Print)

Let's go back to January 2014 when Grantland published an article that outed a trans* woman.[2] This article was nominally about a golf putter and its claims of scientific superiority. However, the article turned into an investigation into the creator of the putter; investigations that dove into her background and ultimately "uncovered" her transition.[3] All of this was part of an article that was meant to evaluate the claims of the science of the putter, not the scientist.[4]

One of the most terrifying parts of the Grantland article is that this type of investigation into a person's background is acceptable practice in journalism if someone becomes a "public" figure. These types of investigations are also an ever-present threat for trans* people through background checks by employers, financial institutions, health insurance providers, and other social institutions. This threat from background investigations makes identity management, privacy, and security difficult for trans* communities. It is this reality that remains excluded from digital security resources—even ones that claim to directly address the needs of trans* communities.[5]

Below I'll go through two examples to highlight the difficulties and nuances of identity management for a trans* person. These examples are based on real situations, but are composites of multiple examples to protect anonymity.

Case 1: Closeted Trans* Person

The internet provides some great opportunities for closeted trans* persons to explore new identities (as the adage from 1993 goes: "On the internet, nobody knows you're a dog").[6] However, there has been an increasing trend in social media and other online communities to verify identities and prevent anonymous users. One prominent example is Facebook's "real name" policy. Often these policies require submission of government-issued identification in order to reinstate an account or verify identity.

[2] http://grantland.com/features/a-mysterious-physicist-golf-club-dr-v/

[3] I won't go into a critique of the Grantland article and its institutional failure. However, the response from the editor and critique from a reporter at ESPN, Grantland's parent company, provide no confidence that Grantland, as a media organisation, understands concerns regarding identity for trans* people.

[4] This sentence purposefully borrows language used early on in the article when Caleb Hannon introduces the first communication with Dr V. In that communication she clearly states her willingness to be interviewed only if the focus is on the science, not the scientist. Her reasons were explicitly noted as concern for safety.

[5] This article should not be seen as bashing any of the resources mentioned. They are good resources and provide a lot of helpful information. However, they are not directed towards trans* persons and do not directly address their needs for digital security.

[6] This adage comes from a 5 July 1993 cartoon by Peter Steiner published in the *New Yorker*.

Trans* people face a great deal of emotional distress due, in part, to a fragmentation of and/or non-representative identities. For a closeted trans* person, this emotional distress is present, but the comfort that comes from coming out publicly as trans* might not be present—only a feeling that a different type of identity provides help.[7] In these situations, one thing that a closeted trans* person can do is to experiment with identities and identity presentations. Their digital identity can be moulded to how they want to be perceived with little to no relation to their birth identity. They might even transition into this identity.

Imagine you are a closeted trans* person using Airbnb, a social room rental service, while traveling. This decision may have arisen out of cost considerations and the ability to present yourself to your host in the manner that you choose. You are careful in the hosts you select and use Airbnb when traveling with trusted friends to rent out an "entire home" to prevent any potentially awkward encounters with the host. Then, out of the blue, Airbnb asks you to verify your identity shortly before you begin a trip.[8] The only way to verify your identity is to send in a government issued Identity Document (ID)[9] to their 3rd party vendor, Jumio. If you don't verify your identity, your current reservations will be cancelled and your account will be deactivated.

What do you do in this situation? You know your ID does not have the same information you've included in your Airbnb profile. If your account gets deactivated, then you will have to book through another service at a much higher financial cost. In this situation, the biggest concern is being outed. There is no transparency around who has access to verification information at Jumio and Airbnb. Sending your data to Jumio would require some explanation of name differences without the guarantee that it would be accepted. Is that information available to Jumio's other clients who use them to verify identities? Even if your account gets reactivated, will Airbnb protect your privacy and rights as a trans* user?[10]

The available resources I have reviewed do not provide any assistance in the creation and maintenance of identities in a way that is trans* inclusive (in some instances despite their claims).[11] The threat model that is addressed in these resources is typically

[7] It is also important to note that a trans* person might choose to not publicly identify as trans*. Even though the example focuses on trans* people who will likely transition, the situation is still applicable to trans* people who choose not to be public about their identity.

[8] According to Airbnb, they have been asking random users to verify their identity since 30 April 2013.

[9] For more information about Airbnb's verification process, see their help centre page.

[10] Despite advertisements and marketing material directed towards the US trans* community (e.g. Airbnb's 2015 ad for the ESPYs in support of Caitlin Jenner, which is now removed from YouTube), their practices seem to indicate a lack of understanding and training against trans* discrimination. See, for example, their handling of a host who rejected Shadi Petosky.

[11] Perhaps the most egregious example of this is Tactical Technology Collective (TTC)'s "Zen and the Art of making Tech Work for You" guide, which explicitly claims to be for trans* activists. However, they use language that can be hostile to trans* identities. In the context of preventing online trolling, creating a fake identity for use in online social media makes sense. However, it does not apply to

the creation of a new/fake identity to insulate activists attacked by online trolls and misogynistic movements, such as Gamergate. While a valid and important threat model, it is very different from the needs for trans* people.

In *The Smart Girl's Guide to Privacy*, Violet Blue (2015) provides some information about protecting data when sending in an identity document. However, it is under the assumption that the service you are sending your ID to, already has your information. In particular, Blue (2015) is writing about the need to send in a government ID to get information removed from people searcher sites. In addition, the available guides are primarily written for laptop or computer use. Some of the guides will go so far as to recommend installing a new operating system that is oriented for security through isolation—a big request of an average user.

The reality of being trans* in the US includes lost economic opportunities. Part of this is related to marginalisation and bias in the hiring process. However, there is also the fact that hormone therapy and gender confirmation surgery cost a lot of money and are not always covered by insurance.

What all of this equates to, is a different perspective—one that these guides ignore in their framing (including intended threats, access to technology, and so forth) and intended audience.

Case 2: Transitioned Trans* Person

This second example might seem more familiar. It is the story of a person who has transitioned and is no longer using their birth name in public.[12] Depending on their situation, they might have undergone hormone therapy and/or gender confirmation surgery. They have removed all the pictures and references to their birth identity that they could. However, there is still information connecting them to their past—snippets, like where they went to school or shared connections—because they didn't want to create a fake identity, but transition into a new one. A number of years after transitioning, someone posts on social media asking if this trans* person is someone they knew from high school and uses their birth name. This is extremely concerning, because even though they have transitioned, they don't want people knowing their birth identity lest it be used as a form of harassment.[13] What are they to do? What could they have done to prevent this?

online trans* identities in general, despite claims to do so by the creators of the guide. Even after bringing up this language issue, TTC and the guide creators stand by its claim to be applicable for general trans* identities online.

[12] In these cases, the trans* person could still be closeted with certain groups, such as family.

[13] A recent example of this is when hate speaker Milo Yiannopoulos publicly harassed a trans* woman at an event he was invited to speak at by the University of Wisconsin.

At the moment, there seems to be a lack of resources to address this need. To complicate issues, in the US, there is no federal standard for something like a name change—the procedure(s) vary by the state. Many states require the publication of a name change, putting trans* people at high risk.[14] For example, Washington, DC removed this requirement after it led to the deaths of trans* people.[15]

At a minimum, any resource on digital/information security for trans* people should recognise these legal requirements, the related risk, and provide information or resources to get more information. In addition, organisations focusing on policy in the digital security and privacy space, should ally with trans* focused legal organisations, such as the Transgender Law Center[16] to jointly advocate for reform of legal and digital laws or policies that endanger trans* people.[17]

Recommendations

At this time, the digital security and privacy community has largely ignored trans* communities.[18] Despite trans* community members, the community itself is typically absent from diversity initiatives or community leadership roles. There are also very few trainers in the community who are trans* or work with trans* communities.

Despite this lack of representation, the community claims to be addressing the needs of trans* people. In my experience this is not the case. Below are a few suggestions to reduce trans* marginalisation in digital security and privacy.

- Do not claim to be speaking to or for the trans* community (or any group) if you have not interacted or worked with them. While I would think that this is an obvious point, there are numerous examples of the digital security and privacy community doing just that for trans* people.
- Refrain from using LGBTQIA+: refer to the specific community or communities that are represented. While connected to the previous point, it deserves explicit mention that using LGBTQIA+ (or any variation) is inherently reductive and marginalising. This is the language that is used in policy and by donors—so it

[14] While I learned about this from my work with activists and organisations, Nico Lang published a good piece of the name change process(es).

[15] This was learned from my experience and conversations with trans* activists and organisations in Washington, DC.

[16] https://transgenderlawcenter.org/

[17] For example, Electronic Frontier Foundation (EFF) partnered with the Transgender Law Center to reform Facebook's "real name" policy in addition to their piece on the concerns with Facebook's policy.

[18] I would like to recognise *Aspiration* for their consideration of trans* attendees and concerns at their Non-profit Software Development Summit. It is the only event I have attended in the digital security and privacy (or related) community that has required pronouns on the name tags. Even small steps of inclusion, like normalising pronoun exchange, are missing from most events.

is understandable that it will still be in use. However, the reality in the US and abroad, is that LGBTI[19] typically refers only to gay men. Instead of creating a false impression of shared goals and needs, explicitly state which communities are represented or discussed.

- Build communities that are trans* inclusive. Inclusion and which groups are represented are choices made by a community. When “diversity” initiatives and community events do not include or consider trans* people, they are not trans* inclusive. At a minimum, ensure a code of conduct that addresses typical forms of harassment and anxiety that trans* people face (such as intentional misgendering and anxiety around which bathroom to use).
- Fund work with trans* communities across the globe (including the US). At the moment little to no funding goes to projects, tools or organisations working primarily with trans* communities. Some reasons for this are restrictions to funding work to particular locations and funding descriptions that more readily accept another secure messaging tool than a trans*-focused policy organisation. If the digital security and privacy community wants to support trans* communities, as it claims to do, provide them with financial support.

It must be emphasised that the above suggestions are not enough. The digital security and privacy community needs to start recognising and addressing threat models that are relevant to trans* communities. The trans* communities that I have worked with do not always share concerns or even legal and social risks. Due to the lack of tools or resources aimed at trans* communities, I have found digital security and privacy to require a largely human approach to risk management. In other words, something that varies from person to person.

A good start to building tools and resources that are trans* inclusive is to recognise the complexity of threat modelling for trans* communities. By taking a trans* inclusive approach to Facebook’s real name policy (a form of identity verification), it is clear that the issue is not just with what is considered a “real” name, but also the notion that a government ID is the only way to verify an identity.[20] [21]

Trans* inclusive digital security and privacy inherently means an expansion of how digital identity is discussed. At the moment, the focus is on rigid sandboxing through tools like Qubes OS.[22] While Qubes has a place in digital security and privacy for trans* communities, tools that allow more flexible and permeable identity boundaries and

[19] The acronym LGBTI is used here because it tends to be the most “inclusive” version of the acronym used by donors, policy makers, and human rights organisations.

[20] By including this example of Facebook’s real name policy the article is not implying that people did not take a trans* inclusive approach to campaigning against Facebook’s policy.

[21] See Case 1, above, for a representative anecdote related to this aspect of identity management.

[22] https://www.qubes-os.org.

resources that help manage identities and data that already exist and are potentially outside the user’s control, are also needed.

These recommendations are not the only ways for digital security and privacy to start addressing the needs of and building new tools and resources for trans* communities. I encourage others from trans* communities and who work with trans* communities to speak up and join the conversation to increase the trans* inclusive tools and resources available.

References

Blue, Violet. 2015. *The Smart Girl’s Guide to Privacy*. No Starch Press.

Caleb, Hanna. 2014. Published in Grantland, http://grantland.com/features/a-mysterious-physicist-golf-club-dr-v/.

Lang, Nico. 2016. *For Trans Americans, changing your name can still be a matter of life or death of the name change process(es)*. Quartz.

Steiner, Peter. 1993. Cartoon published in the *New Yorker*, 5 July 1993.

https://transgenderlawcenter.org.

https://www.qubes-os.org.

https://airbnb.