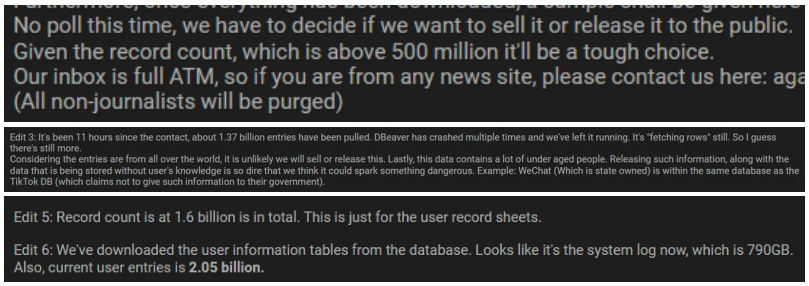
Troy Hunt **@troyhunt** *Sun Sep 04 23:14:33 +0000 2022*

Well this is going to be interesting - has @tiktok_us been breached? **https://t.co/80UGasas1V**

With the preface that all this is "alleged" at this time, there's a post on a popular hacking forum from 12 hours ago making some pretty major claims: **https://t.co/M9oLXhT4Vd**



"There's another DB in the Oracle server we're in, it's called "cabinet cloud" and it's 34GB in total. No idea why it's here and what it's for, but we're releasing it because we don't think we'll need it.

Here's the video of the tables:" **https://t.co/Fw3XAb2fPL**

A 237MB sample was provided which includes the files listed in this Gist: **https://gist.github.com/troyhunt/d238ded80353cce53bea4545545ed172**

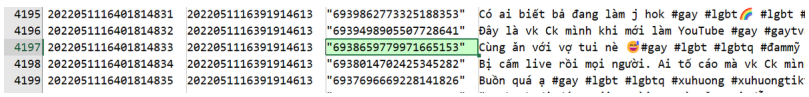
Is it legit? Let's see what's verifiable, starting with the "tiktok_video_username_parse_record_202209032248.csv" file. Looks to be largely Vietnamese LGBT content with IDs, which means we can at least see if they line up with publicly accessible videos... **https://t.co/2mZNDW9xSj**

	"id"	"parse_id"	"video_id"	"video_desc"
2	20220511110817106 19	20220511110805106 18	"6997394725166681371"	Chỉ mong mỗi ngày đều như vậy là hạnh phúc rồi #gay #lgbt #RapperTuTin #dammy #xuhuong #haitie
3	20220511110817106 20	20220511110805106 18	"7094661496214424858"	Làm cục cưng không bé ơi
4	20220511110817106 21	20220511110805106 18	"7094657944431676698"	U là trời nó thôn áaaaaaaaa #haitienofficial
5	20220511110817106 22	20220511110805106 18	"7092714236069072154"	Sang năm anh dắt em về làm dâu
6	20220511110817106 23	20220511110805106 18	"7091286193417014554"	Nhạc hay như tình yêu đầu #gay #lgbtq #dammy #dammy_lgbt #xuhuong #xuhuongtiktok #lgbt🌈 #tren
7	20220511110817106 24	20220511110805106 18	"7090925222995479834"	Đi làm về mệt là những nhẽo à . Thương lắm #gay #lgbt #lgbtq #xuhuong #xuhuongtiktok #trendin
8	20220511110817106 25	20220511110805106 18	"7090584640083348737"	Qua youtube xem ủng hộ tụi em nha của nhà LGBT #gay #lgbt #dammy #dammycongvsthu #bl #lgbtq #l
9	20220511110817106 26	20220511110805106 18	"7087189531719421211"	Thử xin tiền người lạ #gay #lgbt #lgbtq #xuhuong #xuhuongtiktok #trending #trend #dammy #dammy
10	20220511110817106 27	20220511110805106 18	"7085355218455514395"	Làm rằng cho anh Chồng #gay #lgbt #lgbt🌈 #xuhuong #xuhuongtiktok #xuhuong2021 #trend #trendir
11	20220511110817106 28	20220511110805106 18	"7082338760150535450"	Anh yêu em quá trời 🥰🥰 #gay #lgbt #lgbtq #xuhuong #xuhuongtiktok #xuhuong2021 #bl #BL #tren
12	20220511110817106 29	20220511110805106 18	"7082008820456672538"	Cuối tuần cùng vợ chồng Hải Tiến nha #gay #lgbt #lgbtq #xuhuong #xuhuongtiktok #xuhuong2021 #t
13	20220511110817106 30	20220511110805106 18	"7081277536260459802"	Đây là cách chúng tôi bên nhau #gay #lgbt #lgbtq #lgbt🌈 #dammy #dammy_lgbt #xuhuong #xuhuongt
14	20220511110817106 31	20220511110805106 18	"7080551818446572826"	Hai vợ chồng Hải Tiến cùng làm ở công ty #gay #lgbt #lgbtq #lgbt🌈 #xuhuong #xuhuongtiktok #xu
15	20220511110817106 32	20220511110805106 18	"7079436282316721435"	Ước mơ của anh Tiến đã thành sự thật rồi #gay #lgbt #lgbtq #lgbt🌈 #xuhuong #xuhuongtiktok #d
16	20220511110817106 33	20220511110805106 18	"7074586248651820315"	Nhớ em nhiều lắm . Ai yêu thương bé cún mới hiểu được khi mất bé rồi buồn thế nào 😭😭😭😭
17	20220511110817106 34	20220511110805106 18	"7072730864945253658"	Chúc cả nhà 8/3 vui vẻ ạ #gay #lgbt #lgbtq #xuhuong #xuhuongtiktok #haitienofficial

The first entry has an ID that matches this video, and a description that also lines up **https://www.tiktok.com/@haitienofficial/video/6997394725166681371?is_from_webapp=v1&item_id=6997394725166681**

Let's pick a random one a few thousand lines in, Yep, that also matches: **https://www.tiktok.com/@haitienofficial/video/6938659779971665153?is_from_webapp=v1&item_id=6938659779971665**

https://t.co/HBZ6HgWgjR



4195	20220511164018148 31	20220511163919146 13	"6939862773325188353"	Có ai biết bả đang làm j hok #gay #lgbt🌈 #lgbt #
4196	20220511164018148 32	20220511163919146 13	"6939498905507728641"	Đây là vk Ck mình khi mới làm YouTube #gay #gaytv
4197	20220511164018148 33	20220511163919146 13	"6938659779971665153"	Cùng ăn với vợ tui nè 🥰#gay #lgbt #lgbtq #đammỹ
4198	20220511164018148 34	20220511163919146 13	"6938014702425345282"	Bị cấm live rồi mọi người. Ai tố cáo mà vk Ck min
4199	20220511164018148 35	20220511163919146 13	"6937696669228141826"	Buồn quá ạ #gay #lgbt #lgbtq #xuhuong #xuhuongtik

But this is all publicly accessible data so it *could* have been constructed without breach, let's look further...

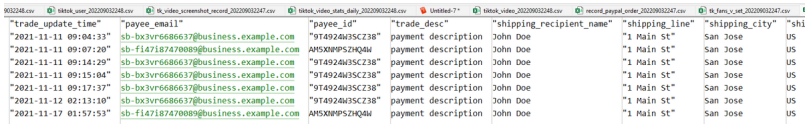
Checking out "tiktok_video_202209032248.csv", the first 2 IDs lead to videos that are no longer available, but the 3rd one returns a hit for an active vid with matching description. Again, scrapable data though... **https://www.tiktok.com/@mxkechong/video/6996802218615655685?is_from_webapp=v1&item_id=6996802218615655685**

https://t.co/VK7xXAbH99

	"row_id"	"id"	"desc"	"create_time"	"origin_cover"
2	1	"6997529256364494085"	This trend a vibe	1629239242	https://p16-sign-va.tiktokcdn.com/obj/tc
3	2	"6997464465310518534"	im falling in love ❤️ #fyp♡ #viral	1629224156	https://p16-sign-va.tiktokcdn.com/obj/tc
4	3	"6996802218615655685"	I beat the odds 😍 #fyp #viral	1629069965	https://p16-sign-va.tiktokcdn.com/obj/tc
5	4	"6996704675818933510"	That snake can die idc 😒 @devin_allen #fyp #viral	1629047254	https://p16-sign-va.tiktokcdn.com/obj/tc
6	5	"6996412041531641094"	Since when 🤷 #foryou #viral	1628979120	https://p16-sign-va.tiktokcdn.com/obj/tc
7	6	"6997529256364494085"	This trend a vibe	1629239242	https://p16-sign-va.tiktokcdn.com/obj/tc

Still need non-public data for verification, so let's look at "record_paypal_order_202209032247.csv". SKU translation here is "15 yuan/100 Tiktok live viewers" and IP addresses are private range. Bit inconclusive. **https://t.co/jzS8qv2req**

Let's look at it the other way - is there anything in there that's obviously fake? Yes, in "record_paypal_order_trade_202209032247.csv": **https://t.co/KfEsmkTRkD**



"trade_update_time"	"payee_email"	"payee_id"	"trade_desc"	"shipping_recipient_name"	"shipping_line"	"shipping_city"	"shi
"2021-11-11 09:04:33"	sb-bx3vr6686637@business.example.com	"9T4924W35CZ38"	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-11 09:07:20"	sb-fi47i8747008@business.example.com	AM5XNMPSZHQ4W	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-11 09:14:29"	sb-bx3vr6686637@business.example.com	"9T4924W35CZ38"	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-11 09:15:04"	sb-bx3vr6686637@business.example.com	"9T4924W35CZ38"	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-11 09:17:37"	sb-bx3vr6686637@business.example.com	"9T4924W35CZ38"	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-12 02:13:10"	sb-bx3vr6686637@business.example.com	"9T4924W35CZ38"	payment description	John Doe	"1 Main St"	San Jose	US
"2021-11-17 01:57:53"	sb-fi47i8747008@business.example.com	AM5XNMPSZHQ4W	payment description	John Doe	"1 Main St"	San Jose	US

Same with "sys_user_202209032248.csv": **https://t.co/KBf2PgBcCx**

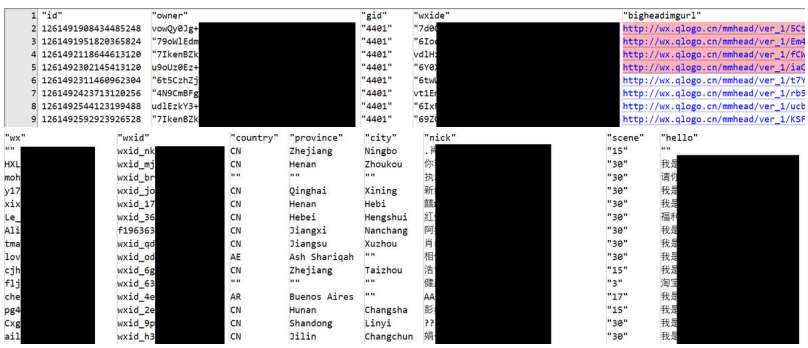
"id"	"user_id"	"login_name"	"user_name"	"role_key"
1	1391683816254091161	testTiktok	testTiktok	
2	1391683816254098709	test25	李婷	
3	1391683816254102563	test26	刘博	
4	1391683816254102793	test27	孙浩楠	
5	1391683816254103096	test28	王兆瑞	
6	1391683816254103278	test29	杨彬	
7	1391683816254836329	闫滕	test30	
8	1391683816254836377	亮亮	test31	
9	1391683816254836388	赵小滨	test32	
10	1391683816254770688	Tiktok监测员	tiktok_monitor	

This is so far pretty inconclusive; some data matches production info, albeit publicly accessible info. Some data is junk, but it could be non-production or test data. It's a bit of a mixed bag so far.

Onto the next data set which is alleged to have from @WeChatApp and is sits alongside the TikTok files. Here's what's in this corpus: **https://gist.github.com/troyhunt/10713b370f0fb01ae704b9aa1357a496**

@WeChatApp The 3 "wechat" prefixed files seem like the most logical place to start, but they're all empty save for column headings: **https://t.co/uHffFbFsHl**

@WeChatApp Let's look at the largest files instead, the top 17 all beginning with "user_friend_request_202209032229_[int]". Obfuscating anything I'm not confident isn't personal, the URLs return avatars and the nicks seem viable at a glance. **https://t.co/uzHr1XQgVb**

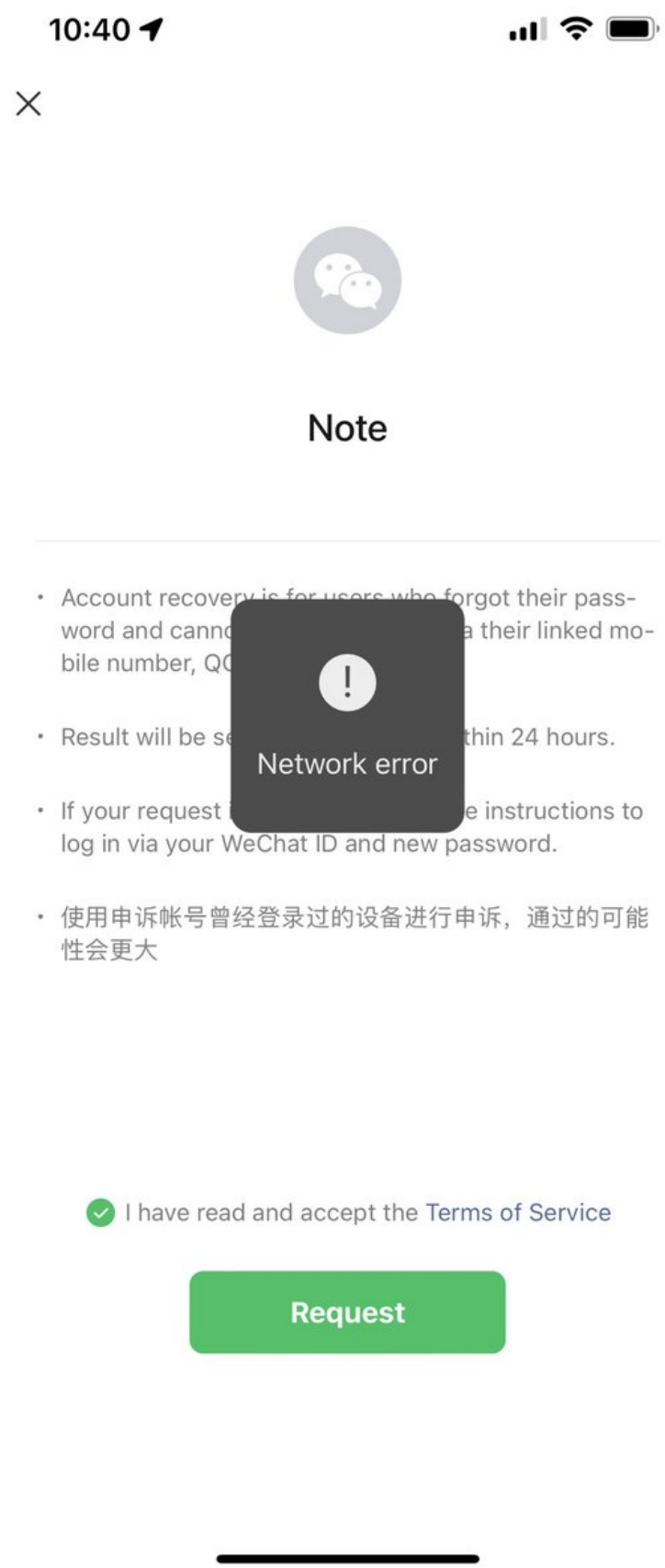


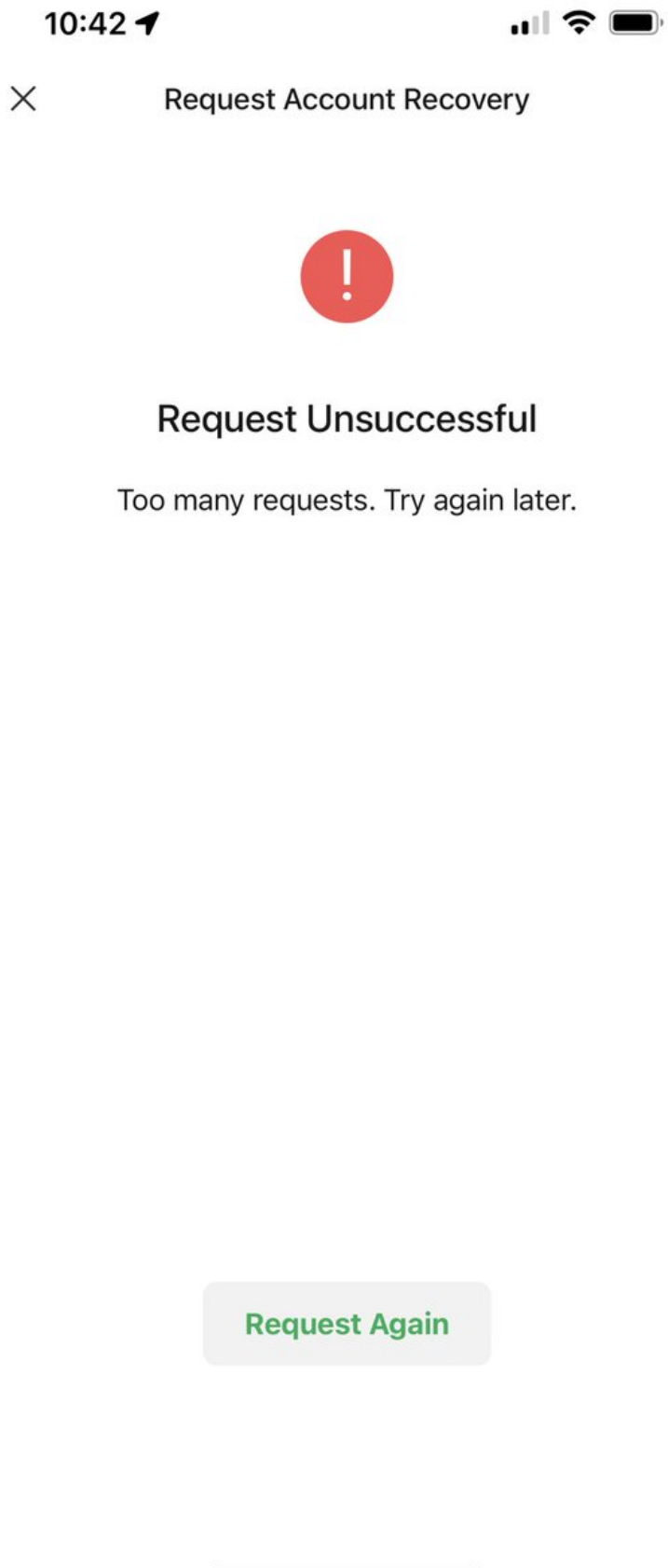
"id"	"owner"	"gid"	"wxide"	"bigheadimgurl"
1261491908434485248	vowQy0Jg+	"4401"	"7d0	http://wx.qlogo.cn/mmhead/ver_1/5Ct
1261491951820365824	"79oWlEdm	"4401"	"6Ioc	http://wx.qlogo.cn/mmhead/ver_1/Em4
1261492118644613120	"7IkenBZk	"4401"	vdlHz	http://wx.qlogo.cn/mmhead/ver_1/fCw
1261492302145413120	u9oUz0Ez+	"4401"	"6Y0	http://wx.qlogo.cn/mmhead/ver_1/iaC
1261492311460962304	"6t5CzhZj	"4401"	"6tw	http://wx.qlogo.cn/mmhead/ver_1/t7Y
1261492423713120256	"4N9CmBFg	"4401"	vt1E	http://wx.qlogo.cn/mmhead/ver_1/rb5
1261492544123199488	udlEzkY3+	"4401"	"6IX	http://wx.qlogo.cn/mmhead/ver_1/ucb
1261492592923926528	"7IkenBZk	"4401"	"69Z	http://wx.qlogo.cn/mmhead/ver_1/KSF

"wx"	"wxid"	"country"	"province"	"city"	"nick"	"scene"	"hello"
""	wxid_nk	CN	Zhejiang	Ningbo	.	"15"	""
HXL	wxid_mj	CN	Henan	Zhoukou	你	"30"	我是
moh	wxid_br	""	""	""	抗	"30"	请你
y17	wxid_jo	CN	Qinghai	Xining	新	"30"	我是
xix	wxid_17	CN	Henan	Hebi	囍	"30"	我是
Le_	wxid_36	CN	Hebei	Hengshui	红	"30"	福
Ali	f196363	CN	Jiangxi	Nanchang	阿	"30"	我是
tma	wxid_qd	CN	Jiangsu	Xuzhou	肖	"30"	我是
lov	wxid_od	AE	Ash Shariqah	""	相	"30"	我是
cjh	wxid_6g	CN	Zhejiang	Taizhou	浩	"15"	我是
flj	wxid_63	""	""	""	健	"3"	淘宝
che	wxid_4e	AR	Buenos Aires	""	AA	"17"	我是
pg4	wxid_2e	CN	Hunan	Changsha	影	"15"	我是
Cxg	wxid_9p	CN	Shandong	Linyi	??	"30"	我是
ail	wxid_h8	CN	Jilin	Changchun	婧	"30"	我是

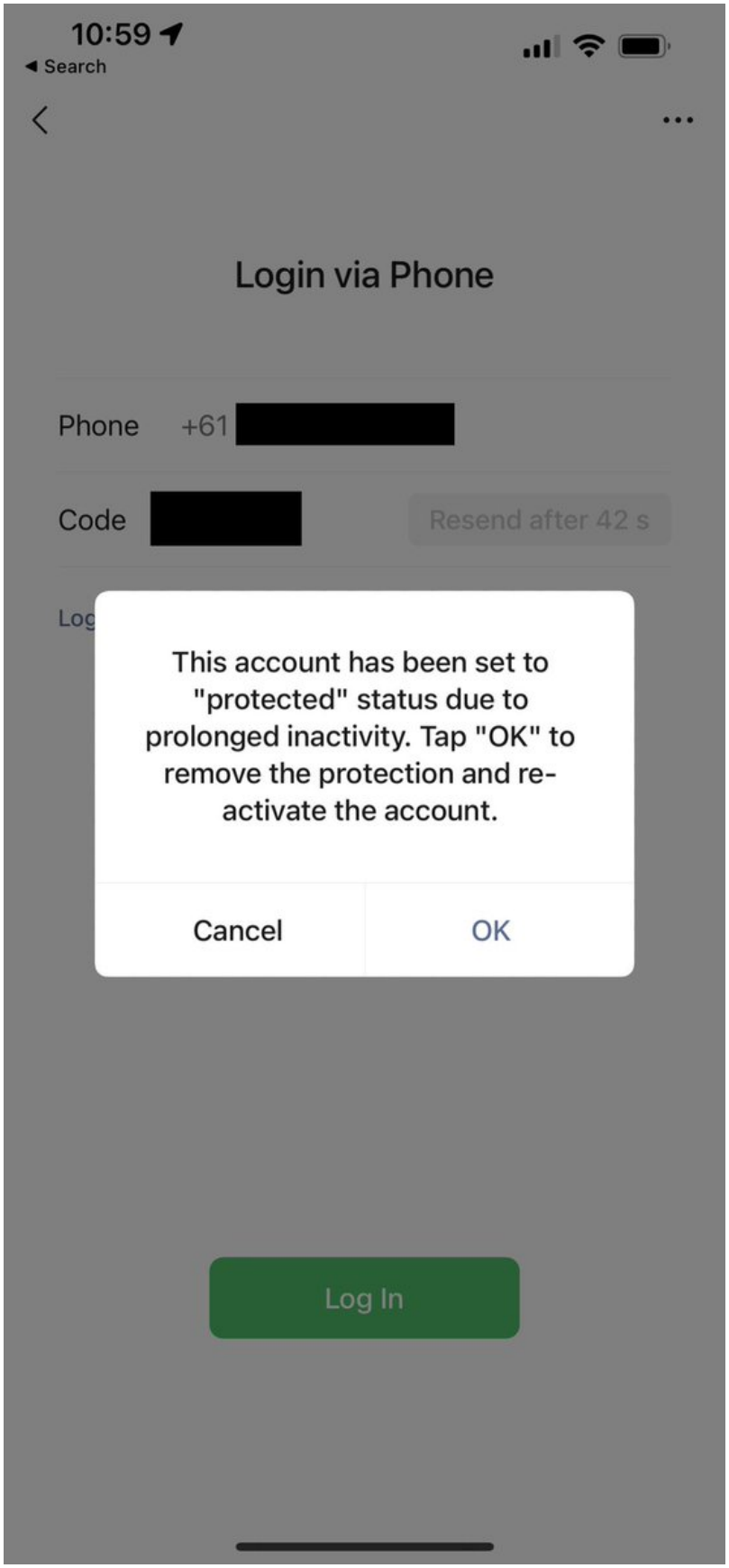
Little trickier verifying as everything is run through the mobile app. No probs, I've got a WeChat account from previous time spent in China. But I used to just login with mob number and now it wants a password. Ok, I'll just recover the

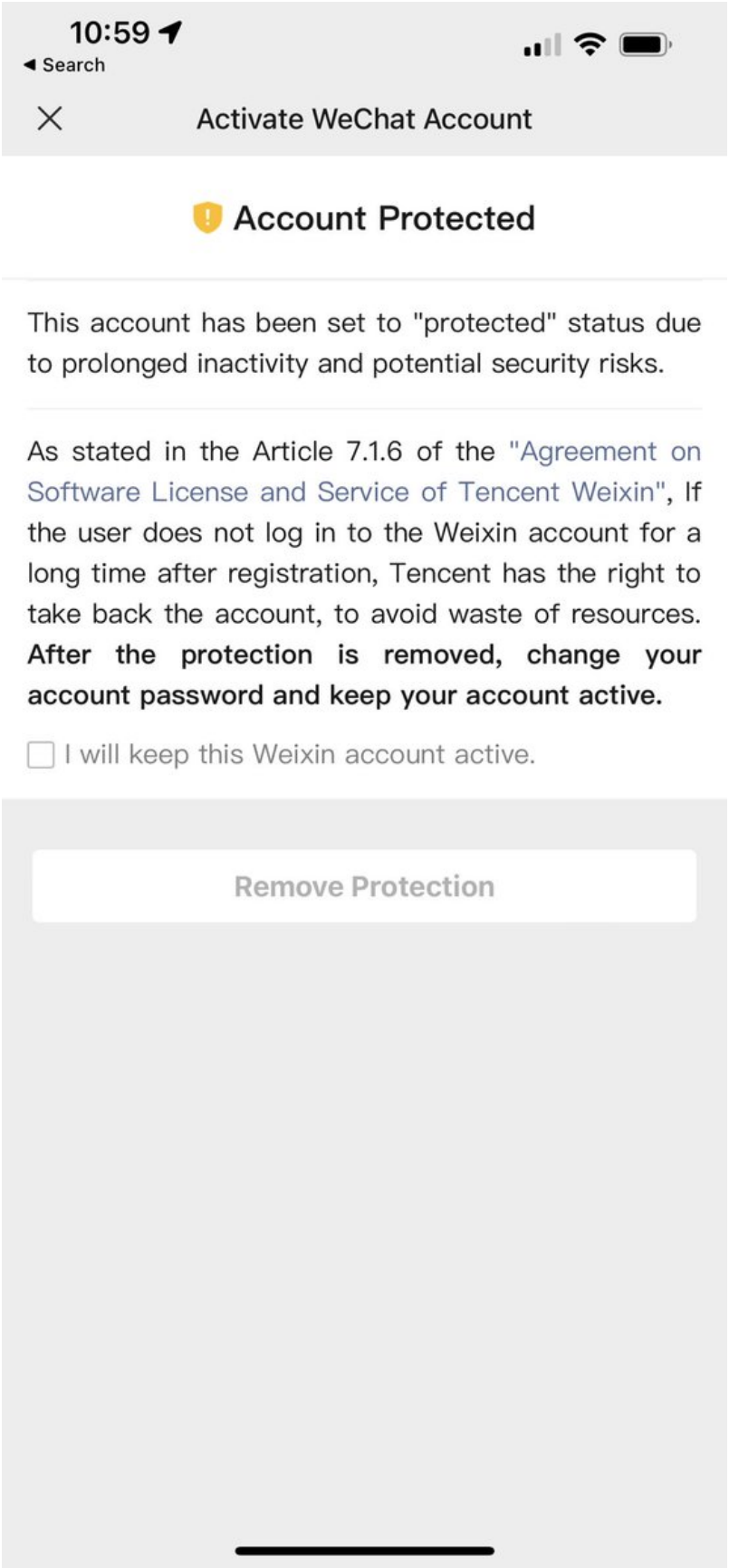
accou… ■■■■ **https://t.co/y6kiyGonRK**





Oh FFS, what an abysmal, completely pointless UX ■■■■ **https://t.co/bPA4Q503qw**


10:59
Search
Login via Phone
Phone +61
Code
Resend after 42 s
This account has been set to "protected" status due to prolonged inactivity. Tap "OK" to remove the protection and re-activate the account.
Cancel
OK
Log In


10:59
Search
Activate WeChat Account
Account Protected
This account has been set to "protected" status due to prolonged inactivity and potential security risks.
As stated in the Article 7.1.6 of the "Agreement on Software License and Service of Tencent Weixin", If the user does not log in to the Weixin account for a long time after registration, Tencent has the right to take back the account, to avoid waste of resources. After the protection is removed, change your account password and keep your account active.
I will keep this Weixin account active.
Remove Protection

11:00

◂ Search

This account is under protection. You can activate it to log in.

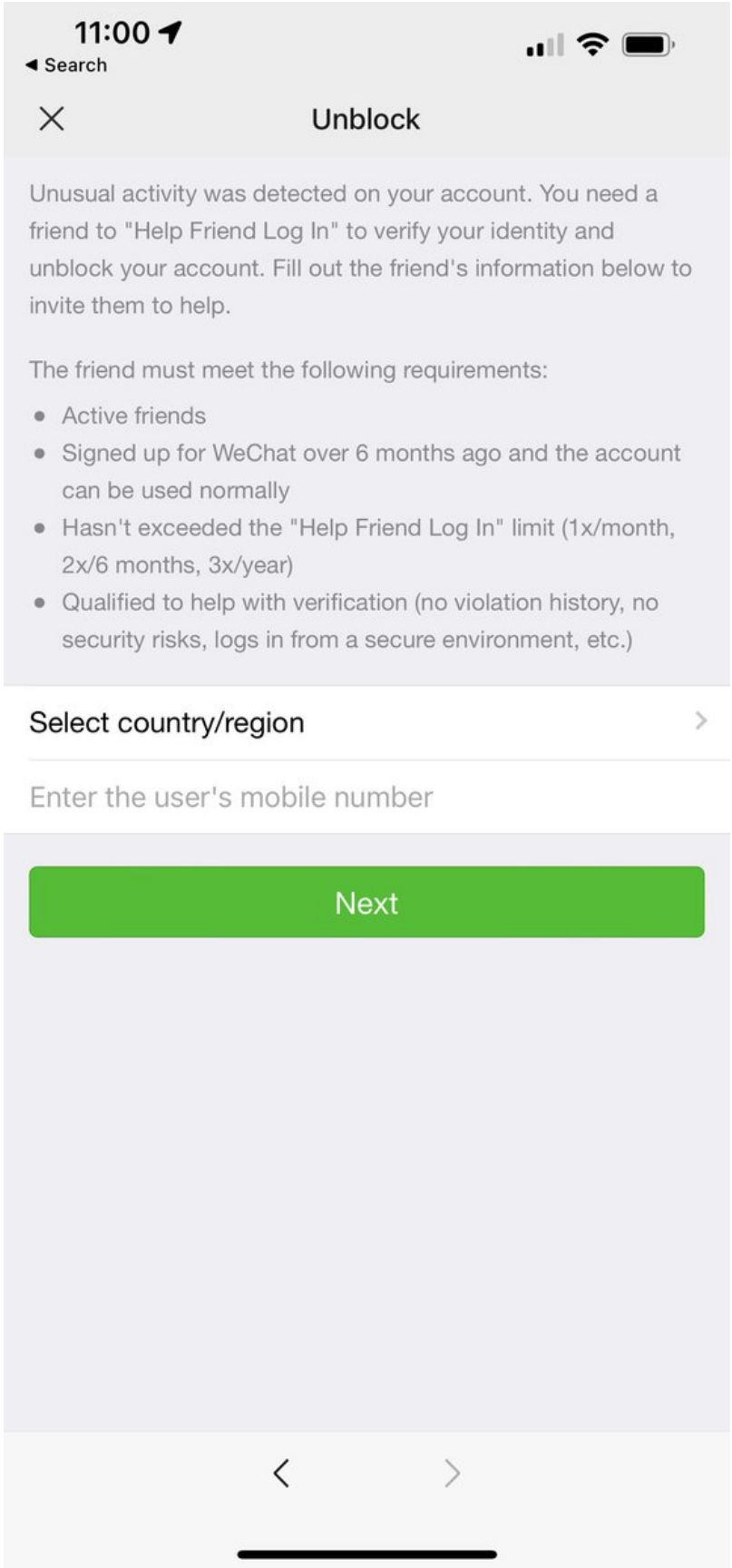
Account  troyhunt

Reason Haven't logged in to WeChat for an extended period

This account has been set to "protected" status due to prolonged inactivity. After activating, make sure you use the account regularly.

Reqeust to Activite Account

Withdraw Funds



Not going to be able to go much further with WeChat without access to the service. It's not clear why this is bundled in with TikTok, AFAIK they're both independently operated entities (government control aside). I find it odd they're presented together, and it's not clear why.