

## GDPO Situation Analysis

June 2015

# From Dealer to Doorstep - How Drugs Are Sold On the Dark Net

Alois Afilipoaie and Patrick Shortis

### Subject

The growing trade in narcotics being sold over the Tor Dark Net is causing academics, law enforcement and policy makers to reassess the impact of ICT technology on real-world crime. Despite growing media attention there are many misconceptions about the difficulty involved and technical knowledge required to participate in these markets and successfully make a sale or purchase. This Situation Analysis aims to explain some of the common practices that vendors and customers alike undertake in order to conduct a secure purchase or sale.

### The Common Starting Point: Computer Security

Regardless of buying or selling, both parties must first ensure their computer system is properly secure before engaging in illicit activity. An average internet user leaves data trails that law enforcement can follow and therefore understanding how to obfuscate or remove these trails altogether is a constant concern of Dark Net market participants. Tor<sup>1</sup>, Bitcoin<sup>2</sup> and PGP (Pretty Good Encryption)<sup>3</sup> encryption are three key technologies that allow successful participation in Dark Net markets.

- Tor - Makes tracking a user via their IP address very difficult by bouncing encrypted data through relays prior to their intended destination.
- Bitcoin - Allows members to use a currency that is difficult to trace to a real-world identity and easy to launder online.
- PGP - Allows messages that might be intercepted by third parties to remain unreadable by anyone who is not the intended recipient of the message, rendering attempts to intercept and read messages between users extremely difficult. It also serves as an important identity-verification tool between users.

1 The Tor Project. (2011). *Overview of Tor*. Available online: <https://www.torproject.org/about/overview.html.en#whyweneedtor> [Last accessed: 10/04/2015]

2 Bitcoin.org. (2009). *How Does Bitcoin Work?*. Available online: <https://bitcoin.org/en/how-it-works> [Last accessed 10/04/2015]

3 pgpi.org. (No Date). *How PGP Works*. Available online: <http://www.pgpi.org/doc/pgpintro/> [Last accessed 10/04/2015]

Understanding these fundamentals represents the first obstacle to successfully participating in the markets. For customers, even a poor understanding of Tor and Bitcoin will still allow most users to make successful purchases, as not all vendors demand that messages are encrypted via PGP. However most serious vendors who engage in daily business will expect PGP utilisation and those who deal in high-demand products will often not read a customer's order without encryption.

Security doesn't stop there. Whilst customers may be able to be lax in their security procedures if ordering small amounts infrequently, most vendors and consistent customers are careful in taking extra precautions such as using a Virtual Private Network to further obfuscate their identity or installing specialised operating systems that reduce their chances of leaving a data trail and wipe all traces of their Dark Net activity after use. The leaks of Edward Snowden demonstrated the far-reaching capabilities of agencies such as the National Security Agency (NSA) and GCHQ and showed that Apple<sup>4</sup> and Windows operating systems can be targeted for exploitation and may even have back doors built into programmes for the purposes of monitoring activity with the knowledge of the developers<sup>5</sup>. They also demonstrated that both agencies worked to deanonymise Tor users<sup>6</sup>. Therefore many users now tend to trust open-source operating systems such as Linux-based operating systems like Whonix<sup>7</sup>. Another popular choice for using Tor is The Amnesiac Incognito Live System (TAILS)<sup>8</sup> which can be installed and ran from a USB storage device or a DVD in order to avoid leaving traces on a user's hard drive and wipes all traces of activity after use. Vendors will also consider whole-disk encryption of their hard drives so that if law enforcement seize their computer they are unable to find evidence of their activity without a password.

There are far more complexities to computer security than can be outlined in this Situation Analysis, and many of them can be found on market forums and knowledge exchanges like The Hub<sup>9</sup>. Technologies like these are what give vendors and customers alike the confidence to feel secure in their activities, especially when leaked documents from the NSA consider the combined use of systems like Tor, TAILS and PGP to be 'catastrophic' and resulting in 'near-total loss/lack of insight to target communications [and] presence'<sup>10</sup>.

## Acquiring Bitcoin

Since the majority of Dark Net marketplaces only accept Bitcoin<sup>11</sup>, customers must acquire some in order to purchase. This is done by exchanging fiat currency such as dollars, Euros or pounds into Bitcoin through online exchange markets such as BitStamp and BTC-E<sup>12</sup>. Some exchange markets such as BitStamp have very strict 'Know Your Customer'<sup>13</sup> policies intended to link real-world identities to Bitcoin transactions, whereas others such as BTC-E, BitFinex and BTC China require minimal to no identification at all in order

4 Greenwald, G. MacAskill, E. (2013). *NSA Prism program taps in to user data of Apple, Google and others*. Available: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> [Last accessed 10/04/2015].

5 Greenwald, G et al. (2013). *Microsoft handed the NSA access to encrypted messages*. Available online: <http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> [Last accessed 10/04/2015]

6 Electronic Frontier Foundation. (2014). (GCHQ Leak) *A Potential Technique to Deanonymise Users of the TOR Network*. Available: <https://www.eff.org/document/20141228-speigel-potential-technique-deanonymise-users-tor-network> [Last accessed 10/04/2015]

7 Whonix.org. (2009). *Whonix: About*. Available: <https://www.whonix.org/wiki/About>. [Last accessed 10/04/2015].

8 TAILS. (2015). *The Amnesiac Live Incognito System*. Available: <https://tails.boum.org/>. [Last accessed 10/04/2015].

9 The Hub (Unknown). *(Only Accessible Via Tor)*. Available: <http://thehub7gqe43miyc.onion/> [Last accessed 10/04/2015].

10 Der Spiegel Staff. (2014). *Prying Eyes: Inside the NSA's War on Internet Security*. Available Online: *Prying Eyes: Inside the NSA's War on Internet Security* [Last accessed 10/04/2015]

11 For more information on Bitcoin see the GDPO's Situational Analysis: *The Booming Market of Alternative Cryptocurrencies*. Available online: [http://www.swansea.ac.uk/media/Crypto\\_SA.pdf](http://www.swansea.ac.uk/media/Crypto_SA.pdf) [Last accessed 10/04/2015]

12 There are also other methods of acquiring Bitcoin such as a direct transaction with another user of the crypto-currency.

13 Requiring registered users to present a number of identification documents such as full address documentation together with proof of residency as well as photographs

to open an account<sup>14</sup>. Once registered with an exchange the user will trade their fiat currency for bitcoins. However as it is not advised to either leave the bitcoins in the deposit of a Dark Net market or to store bitcoins online due to the high risk of theft, the user would then download a bitcoin client such as Bitcoin Core or Armory<sup>15</sup> and import the cryptocurrency from the online exchange to the bitcoin client situated on the user's computer. The bitcoin client would also generate a bitcoin wallet which will be used to send and receive bitcoins. The existence of a bitcoin wallet also allows the user to directly add credit to their account without the use of bitcoin exchanges and through the use of bitcoin ATMs which permit inserting cash to credit a person's bitcoin wallet<sup>16</sup>.

Vendors too must acquire bitcoins using similar methods in order to pay the fees necessary to open a vendor account. Fees vary from site to site with the popular markets such as Evolution<sup>17</sup> or Agora charging 1 BTC and 1.5 BTC respectively whilst smaller markets charge as little as \$50.<sup>18</sup> Setting vendor fees ensures that markets can profit from participation, whilst ensuring that vendors are invested in doing reputable business and scammers are deterred from setting up fake vending accounts in order to prey on inexperienced customers.

## Prior to purchase

### *Setting up the store*


In order for vendors to successfully make a sale they must set up their store front. Paying their vendor fees to their intended site is the first step and fees can differ from market to market. Once the account is secured then vendors provide their 'blurb' about themselves and their products, as well as useful information such as feedback policies, offers and bulk discounts they may provide (See Box 1). Most vendors who expect consistent business also create brand identity and may even invest in marketing via offering free samples to be reviewed by customers in order to kick-start a positive review feed.<sup>19</sup>

#### **Box 1: A vendor advises another to buy ecstasy tablets in bulk as they sell quickly**

Anymore, the way I see it, if I'm ordering Xpills international, might as well make the order worth it so you don't have to repeat it every two weeks.

Grab 200+, 'cause once your custies get a taste for dank xpills, that's all they'll want and they go way faster than xtal MDMA.

Sometimes I look at those listings that say 10,000 xpills, makes me salivate, jelouse, wish I had the btc to cop that shit, I'd be set for a few months.

Report to moderator 

("Xpills" = Ecstasy pills, "custies" = Customers "btc" = Bitcoin)

14 Data provided by The Merkle. (2014). *Best Bitcoin Exchange: which BTC/USD exchange is the best?* Available online: <http://themerke.com/reviews/best-bitcoin-exchange/> [Last accessed 10/04/2015]

15 Pieces of software which allow for direct transactions between user accounts without any third party involved

16 Coindesk. (2014) *How to store your Bitcoins*. Available: <http://www.coindesk.com/information/how-to-store-your-bitcoins/> [Last accessed 10/04/2015]

17 In the course of developing this paper this market was closed by staff, stealing millions of dollars of bitcoins in the process.

18 DeepDotWeb. (2015) *Dark Net Markets Comparison Chart*. Available Online: <http://www.deepdotweb.com/dark-net-market-comparison-chart/> [Last accessed 10/04/2015]

19 For more information on marketing see GDPO Situational Analysis: *The Growing Industry of Dark Net Marketing*. Available: <http://www.swansea.ac.uk/media/GDPO%20SA%20Marketing.pdf> [Last accessed 10/04/2015]

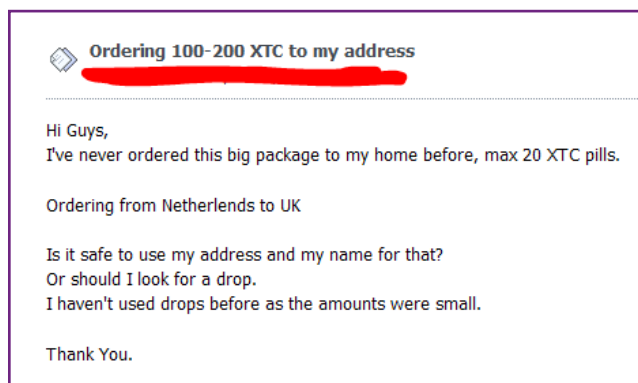
How vendors acquire stock is obviously difficult to ascertain, however there is strong evidence to suggest that whilst some will source from street-level dealers to sell online, many are actually using Dark Net markets to buy bulk amounts of product then sell it in smaller more profitable quantities in their local areas for a profit. This has been characterised as being a 'transformative Criminal Innovation'<sup>20</sup> and is supported by anecdotal evidence in interviews with participants<sup>21</sup> as well as conversations on forums.

For serious vendors, Dark Net sales are their key business and their business model is in many ways comparable to any small-size internet-based mail-order business<sup>22</sup>. The key features include:

- Address labels, packaging material and key tools such as vacuum-sealing kits are bought in bulk in order to accommodate the regular orders.
- Regular deliveries are dropped off to predetermined post offices in order to avoid attention at one particular place and careful care and attention is taken in ensuring packages look like legitimate mail.
- Ensuring security standards in the handling and packing of drugs in order to avoid any possibility of detection during routine postal inspections with sniffer dogs is a priority. Therefore some vendors will have a packaging 'clean' room with a clearly designed system of packaging which avoids any fingerprints or DNA accidentally being sent as well as any avoiding leaving drug residue on the exterior of packages.

### Customers: Preparing the address and purchase

Prior to purchasing customers will usually consider how they want the delivery made. Some will hire a mailbox for the package to be delivered to if concerned by it being intercepted by police whilst in transit to their home address. There are various guides offered in forums and markets that give users information on how to do this securely. The fear of a 'controlled delivery' is widespread, a scenario whereby law enforcement attend a package delivery and arrests the recipient. Most Dark Net market forums have information on to how best avoid one of these scenarios or what to do when faced by one. Whilst some customers will attain a postal address of a friend or a post box using a false identity, most are happy to have packages sent to their home using their real name. This is considered to be generally safe, especially if purchasing small amounts.



Many customers will also launder their bitcoins prior to purchasing in order to gain more security. This is done to make sure that the bitcoins acquired cannot be traced by law enforcement to the bitcoin exchange market and thus to the buyer's identity. To do this the user would send their bitcoins from their personal wallet to a bitcoin tumbler such as Grams Helix<sup>23</sup> which would tumble the funds and send them back to the user, now with a completely new origin (it is claimed by Grams Helix that these bitcoins are completely new and untouched), thus making it harder for law enforcement to create a link between the bitcoins and the users true identity.

20 Aldridge, J and Décarry-Héту, D (2014) *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation* Available online: <https://www.escholar.manchester.ac.uk/api/datastream?publicationPid=uk-ac-man-scw:253395&datastreamId=FULL-TEXT.PDF> [Last Accessed: 10/04/2015]

21 Fox-Brewster, T (2015). *Astonishing Images Show \$4.2 Million In Seized Dark Market Drugs*. Available Online: <http://www.forbes.com/sites/thomasbrewster/2015/03/13/shiny-flakes-bust-pictures/> [Last accessed 10/04/2015]

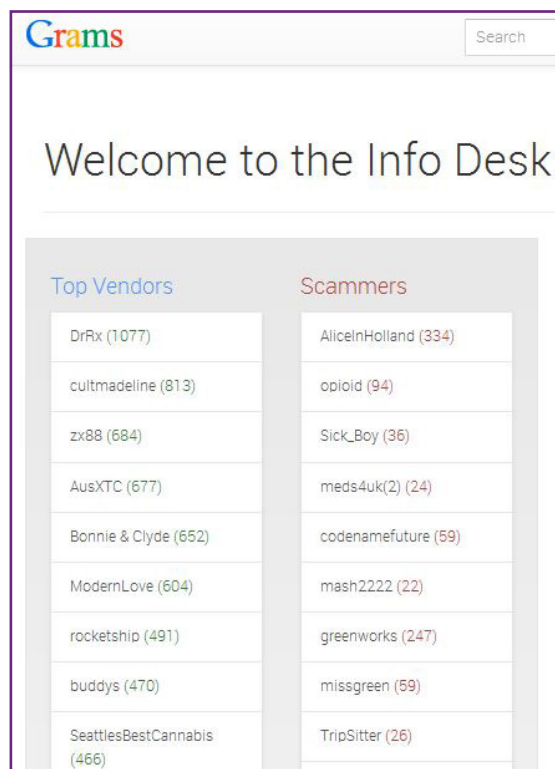
22 Berkman, Fran. (2013). *Exclusive: Inside the World of a Silk Road Drug Dealer*. Available Online: <http://mashable.com/2013/10/02/silk-road-drug-dealer-interview/> [Last accessed 10/04/2015]

23 As explained in the GDPO's Situational Analysis: *The Booming Market of Alternative Cryptocurrencies*. Available online: [http://www.swansea.ac.uk/media/Crypto\\_SA.pdf](http://www.swansea.ac.uk/media/Crypto_SA.pdf) [Last accessed 10/04/2015]

## The Purchase

There are a number of rules that ensure that the transaction between vendor and buyer is safe and successful for both parties:

**Reviews** - As no one desires to be scammed and receive a low-quality product or experience delays in delivery, a review system assesses the quality of product and trustworthiness of a vendor. Review systems can be found on all popular markets, however Dark Net search engine Grams has created a list of vendors from most active Dark Net marketplaces and the Infodesk service presents both the top vendors as well as the scammers, according to the cumulative quality of reviews they receive on their various marketplaces. The review system is a critical tool for informing customers and it is emphasised by the administrators of most marketplaces to read them before purchasing. Similarly some markets offer the chance for vendors to review customers in order to differentiate serious buyers from those who may make false claims about vendors to try and initiate a refund through the escrow system. customers would usually write a review of their own describing the quality of the product and delivery time as well as rating the vendor on a scale of 1-5 or awarding positive, neutral or negative feedback (as shown on Evolution above).



Top Vendors	Scammers
DrRx (1077)	AlicelnHolland (334)
cultmadeline (813)	opioid (94)
zx88 (684)	Sick_Boy (36)
AusXTC (677)	meds4uk(2) (24)
Bonnie & Clyde (652)	codenamefuture (59)
ModernLove (604)	mash2222 (22)
rocketship (491)	greenworks (247)
buddys (470)	missgreen (59)
SeattlesBestCannabis (466)	TripSitter (26)

**The Escrow System** - This is a key trust mechanism which is designed to prevent scamming. In this system the buyer would transfer bitcoins from their desktop wallet to their wallet on the marketplace they are purchasing from. At the point of purchase the funds are moved from the buyer's marketplace wallet and into

+	Next day delivery no complaints been coming for months always good quality product good prices, all round good vendor	r***5
+	As always, quick delivery and great stuff. FE for trusted vendor	m***4
+	No comment.	d***j
+	Great vendor would recommend! Stealth was good and sent 2.25g when I ordered 2, which is always nice! The product it's self was great, didn't test purity but I'm sure it is what he claims or very close! Will buy again in future	j***6
+	Amazing product, great vendor and perfect stealth. Tested with Marquis, Mandelin, Mecke, Simon's and Robadope reagents. Probably the highest quality MDMA I have ever had, and it was very nicely over-weight. I will diffinatly be using this vendor again.	m***s
+	As previous purchase, was received quickly and with good stealth. Amount and quality both seemed spot on to me. Keep up the good work - I'll definitely be a regular customer with this vendor.	p***t

the escrow system, a wallet run by the site. The vendor is notified the funds are in the escrow and begins the process of delivery. The delivery address is provided by the buyer through a PGP encrypted message which only the vendor can unlock by using their PGP key<sup>24</sup>. Once the delivery has been made the customer signals the market to release the funds from the escrow to the vendor. In this model the security of both parties is protected with the marketplace itself being the objective third-party that can settle disputes. If the customer is not willing to pay despite receiving product than the money is auto-finalised after a few days to ensure the vendor is paid. There is also a 'finalise early' option (FE) that allows customers to release funds to the vendor before the product has arrived. Some vendors only engage in a transaction if the customer is willing to 'FE' however due to the amount of scams that take place with this method it is generally deemed inadvisable. Some customers do 'FE' for vendors with long-established reputations or for vendors that the customer buys from regularly and trusts.

**Delivery** - Stealth and packaging are two key components to delivery and often impact a vendor's review rating. 'Stealth' refers to how the product is disguised to look like a legitimate delivery item, especially in regards to postal service x-ray machines. Some vendors have sent drugs or contraband hidden in DVD cases, battery compartments of torches and the spines of books in order to disguise it. Packaging refers to how the

<sup>24</sup> Note that this is in a perfect scenario, again many customers will not encrypt their messages which is generally considered poor operational security. See how PGP works here: <http://www.pgpi.org/doc/pgpintro/>

drug is packaged to avoid detection by sniffer dogs or other means of detecting odours and traces. Vendors use Moisture Barrier Bags, vacuum-sealing kits or Mylar bags that are designed to avoid any smell emanating from the package that might be picked up by a sniffer dog whilst also preventing any visual confirmation that the product inside is drugs (bags are opaque). While discussions on stealth and packaging used to be open to all participants on market forums, many contemporary market forums require a vendor account to access these topics in order to deter law enforcement agents from learning techniques.

## Laundering the Bitcoin II

Due to the nature of how Bitcoins transactions work, change is usually given at some point in the process<sup>25</sup>. This change, originating from the Dark Net market's escrow would be automatically deposited back to the buyer's wallet on their desktop client. With thorough blockchain analysis the origin of these Bitcoins, however, could be traced and thus, as a security measure, buyers send their bitcoins to a tumbler and receive back clean bitcoins<sup>26</sup>.

Vendors may also consider laundering their profits through a bitcoin tumbler in order to receive clean bitcoins that are hard to link to their true identity. As thousands of Bitcoins can be stored and encrypted onto offline-wallets it can make hiding large sums of money a trivial affair as wallets can be hidden within computers or USB sticks in order to safely store them. However, due to the volatility of Bitcoin it is seen to be more advisable to exchange it for local currency in small but regular amounts to avoid attracting attention from law enforcement agencies.

## What Next?

Whilst the basic processes of buying and selling drugs on Dark Net Markets are largely the same as they were in the early days of the Silk Road, there are several trends that could suggest changes to these methods in the future.

- Memex is a new search engine developed by America's Defense Advanced Research Projects Agency that aims to create a more intelligent search capability for military, law enforcement and academics. Memex indexes sites and data that many other search engines avoid and its capabilities allow it to quickly search through the Deep Web and connect the dots between multiple data sets and then visualise them in a way that is helpful to investigators. So far, it has been used in the fight against illegal human trafficking<sup>27</sup> but the developers have been working with members of the Tor Project and are interested in using Memex as a way to study Dark Net markets and Tor hidden services in general<sup>28</sup>.
- Bitcoin has weaknesses in making illicit transactions due to the publicly available information stored on the blockchain being vulnerable to analysis by law enforcement. However it will remain the most commonly adopted cryptocurrency used on the Dark Net for the foreseeable future<sup>29</sup>. If law enforcement capabilities drastically improved to analyse bitcoin transactions and pin them to individuals in real time with a good accuracy ratio than it is likely that another coin would be adopted, such as Darkcoin, which provides more security features.

25 Coindesk. (2015) *How Do Bitcoin Transactions Work?* Available Online: <http://www.coindesk.com/information/how-do-bitcoin-transactions-work/> [Last accessed 10/04/2015]

26 Again, as mentioned before, bitcoin tumbling is subject to wide debate, but since some see it as a mandatory measure to keep them safe it has therefore been included in this Analysis. Secondly, chances that tumbling would be used twice in the process of a purchase are low, but most buyers would either launder their bitcoins at first or they would launder them last. Nonetheless, there are buyers who for the extra bit of security would launder as often as they can, in spite of the commission asked by such services (0.5%-3%).

27 Greenemeier, Larry. (2015). *Human Traffickers Caught on Hidden Internet*. Available online: <http://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/> [Last accessed 10/04/2015]

28 Zetter, Kim. (2015). *Darpa Is Developing a Search Engine for the Dark Web*. Available: <http://www.wired.com/2015/02/darpa-memex-dark-web/>. [Last accessed 10/04/2015]

29 See GDPO's Situational Analysis: The Booming Market of Alternative Cryptocurrencies. Available online: [http://www.swansea.ac.uk/media/Crypto\\_SA.pdf](http://www.swansea.ac.uk/media/Crypto_SA.pdf) [Last accessed 10/04/2015]

- International and domestic mail centres are obviously key places to try and intercept contraband on its way between vendors and customers. However improving success ratios drastically is difficult without slowing speed of delivery (which could affect commercial interests) or encroaching on civil rights laws that protect an individuals mail from seizure without a warrant. Aside from that, the sheer number of staff, extra x-ray machines and sniffer dogs needed would be a drain on resources that are already being stretched fighting the much larger market for street-level drugs. Therefore, from a law enforcement angle it seems like an unlikely way to combat the Dark Net drugs trade in the long run.
- Markets have been shut down by law enforcement or administrators have stolen all the Bitcoins and closed the sites (as the staff behind popular market Evolution did recently), and this has caused turmoil and uncertainty in trusting centralised marketplaces like Agora, AlphaBay or Middle Earth Marketplace. This turmoil has led to a steady rise in vendor shops where vendors are creating their own mini-market pages and selling independently from these bigger markets directly to their customers. This model will probably continue to grow as more vendors become tired of losing their money to markets with poor security or greedy administrators.
- Technologically this shift is in line with other decentralisation processes in illicit cyber behaviours such as moving from a centralised Napster file-sharing model to decentralised torrent model. We expect to see this in the form of a gradual shift towards Dark Net models like OpenBazaar, which will allow users to set up storefronts individually and greatly limits the ability of law enforcement to undertake mass-market shutdowns like those seen in Operation Onymous.

supported by



### About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

### Global Drug Policy Observatory

Research Institute for Arts and Humanities

Room 201 James Callaghan Building

Swansea University

Singleton Park, Swansea SA2 8PP

Tel: +44 (0)1792 604293

[www.swansea.ac.uk/gdpo](http://www.swansea.ac.uk/gdpo)



@gdpo\_swan

