A New AI Lexicon

Function Creep
Change as a trace of dominant norms

Abstract
Changes in the functionality of algorithmic systems are often described as creep, a technical exception with unwanted and harmful consequences. However, algorithmic systems are built to be multi functional and creep is not merely a technical issue. Therefore function creep is better understood as a modus operandi of algorithmic systems, a testament to their technical mutability and political entanglement. To properly understand change in these systems, they need to be read in relation to existing spheres of power, from the ideological to the algorithmic level.

Originally published in 2021 as part of the AI Now Institute's "AI Lexicon" project, a call for contributions to generate alternate narratives, positionalities, and understandings to the better known and widely circulated ways of talking about AI. The project is now offline.

The functions of a system and the actions it is able to perform change over time. Function creep refers to a specific kind of change: the expansion of the functionality of an algorithmic system, a divergence of its initial purpose and actual use.[1] For example, a system intended for regulating workers' access to company grounds may be repurposed to track attendance or to detect if workers wear face masks and keep distance to prevent the spread of Covid-19.[2]

While there is no commonly agreed on definition, the term is found in AI engineering[3] and policy[4] but also specifically in the discourse around AI fairness, accountability, and transparency[5]. Often, function creep is linked to potential privacy infringements resulting from the use of an algorithmic system. However, the use of the term is not always precise. For example, Andrejevic & Selwyn warn of the potential of face recognition systems: "in terms of function creep, [face recognition is a] technology with a host of potential lucrative markets – from shopping centres wanting to deliver personally-targeted advertisements to shoppers, through to employers wanting to keep tabs on the whereabouts of their workforce."[6]

Such warnings miss a crucial point. Face recognition and other algorithmic systems are built to be repurposed. The possibility to expand the set of functions of these systems is one of their core features. That a repurposing may cause rights infringements should be expected. As Bernal[7] writes, the risk of function creep in commercial and law-enforcement contexts is present whenever data is held. Nonetheless, as will be shown below, function creep is regularly framed as an exception. Instead, function creep is better understood as the modus operandi of algorithmic systems, a testament to their technical mutability and political entanglement.

---

[1] Scope creep and feature creep are also common terms to describe the expanding use of technical systems.

[2] *AI companies repurpose their software for workplace social distancing monitoring*. Privacy International. Retrieved July 22, 2021, from http://privacyinternational.org/examples/4197/ai-companies-repurpose-their-software-workplace-social-distancing-monitoring

[3] For example, in a recent advisory rapport on a Dutch Covid-19 tracing app by De Winter Information Solutions to the Dutch government, the report estimates the likelihood of function creep as low. https://www.rijksoverheid.nl/documenten/rapporten/2020/10/01/duidingsrapportage-coronamelder

[4] For example, the European Data Protection Supervisor (EDPS) uses the term in a post on a workshop on AI and Facial Recognition Challenges and Opportunities. https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en

[5] For example, at the FAccT conference in 2021, when speaking about Covid-19 and immunity passports on the 'Machine Learning and Health' panel, Seda Gürses rightly stated that "you cannot limit mission creep on this". https://www.youtube.com/watch?v=mT_QmoMC2uk

[6] Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology and the end of privacy for good. Monash Lens. https://lens.monash.edu/@politics-society/2020/01/23/1379547?slug=facial-recognition-tech-and-the-end-of-privacy

[7] Bernal, P. (2014). Internet Privacy Rights: Rights to Protect Autonomy. Cambridge University Press.

The Standard View

Most definitions of function creep describe the phenomenon unidimensionally, suggesting that it occurs due to technical properties of a system. For example, Koops states that, "function creep denotes an imperceptibly transformative and therewith contestable change in a data-processing system's proper activity."[8] Here, creep refers to an impactful but previously imperceptible widening of a specific set of functions of a system. This widening may be the result of new functions introduced purposefully by designers or discovered accidentally by users of a system. It can thus refer to intentionally added or unintentionally enabled functions. In both cases, the metaphor of *creep* is invoked to describe an initially imperceptible change towards a new function, with unwanted effects such as privacy or other rights infringements.

To reign in creep, researchers suggest limiting or specifying the use cases of an algorithmic system. Koops proposes that function creep can be prevented by regularly assessing a system's functioning, discussing the effects of possible creep and, if creep occurs, "argue why they think the change is in line with what the system is supposed to do, and where needed, take appropriate measures to make it more acceptable."[9] According to the author, this might mean limiting functions that cause privacy infringements or arguing why these infringements are necessary.

There are also legislative attempts at preventing function creep in algorithmic systems. These focus on the 'purpose limitation principle,' solidified in Article 5(b) of the European General Data Protection Regulation (GDPR). According to this principle, personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[10] In other words, purpose limitation aims to prevent function creep by restricting the use of data to specific and compatible objectives. Yet it is not always clear what constitutes an incompatible purpose and how compatibility is negotiated.

Broad mandates of law enforcement and intelligence agencies allow overruling the principle in the name of national security interests. As a result, law enforcement agencies may be able to access data from other agencies such as immigration services and may also include publicly available data.[11] In these cases, policing measures may turn into surveillance efforts that comply to regulation because of legitimate security purposes.[12] As Kak puts it, these data processing systems are structured to evade and remove the purpose limitations on data use.[13]

Still, some suggestions for limiting function creep suggest hard-coding purpose limitation by restricting functionality. For example, Fantin and Vogiatzoglou[14] call for purpose limitation to be adopted in the design phase of new AI systems. The authors suggest that, by designing an AI for specific use cases only, function creep could be redressed. Specifically, the authors propose that restrictions should be embedded in predictive analytics systems so that they pause in the case of compatibility issues and wait for a human assessment to clear the case. The authors do not take into account that the halting of a system may also

---

[8] Koops, B.-J. (2020). *The Concept of Function Creep* (SSRN Scholarly Paper ID 3547903). Social Science Research Network. https://papers.ssrn.com/abstract=3547903.

[9] Ibid.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1807-1-1

[11] Such as location data from social media. Big Data and Analytics in Law Enforcement: Predictive Policing. (2021). Sintelix. https://sintelix.com/blog/big-data-analytics-law-enforcement-policing/

[12] Fantin, S., & Vogiatzoglou, P. (2020). Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence (SSRN Scholarly Paper ID 3679850). Social Science Research Network. https://papers.ssrn.com/abstract=3679850

[13] Kak, A. (2020). Regulating Biometrics: Global Approaches and Urgent Questions. AI Now Institute.

[14] Ibid.

have unwanted effects on its subjects, e.g. if they need data processing to take place in order to be issued documents. Furthermore, the authors propose that the restrictions for purpose limitation should be separately defined for different types of crime.

It is this approach that encapsulates the standard view on function creep: assuming the benevolent use and complete control over the design and effects of an algorithmic system to an extent where any unintended consequences are exceptional. But this belief, that the use of a system can be controlled by design, is precisely what enables function creep. Understanding and redressing function creep thus requires a different approach.

Functionality is Boundless

Understanding functionality of an algorithmic system in terms of the actual output generated by that system at a specific point in time is insufficient to understand its effects. In particular, two convictions at the core of the standard view of function creep need to be refuted: that a system's functionality can be clearly delineated and that creep is an exception. On closer inspection, the purposes for which algorithmic system is used are not merely stipulated by its technical capabilities. A wider understanding of function creep is necessary.

In the case of machine learning, the functionality of a model is partly derived from its ability to classify a certain input to a satisfying degree of statistical accuracy, e.g. indicated by a high F-score.[15] A model that classifies road signs accurately enough can function in a self-driving vehicle, a model that classifies most tents in satellite imagery correctly can be used to estimate camp population. From an engineering standpoint, it makes sense to describe functionality in these terms.

Yet new functions dynamically arise as systems change.[16] Whether those changes are designed or occur post-deployment matters much less than how the system can be flexibly deployed in real world settings. This is why dual-use technology, suitable for both military and civilian use, is subject to debate and regulation. Furthermore, the functions of an algorithmic system, the purposes for which it *could* be utilised, can creep beyond strictly algorithmic activity. Hypothetical functions of an algorithmic system may well have real effects, without any data being processed.

The emphasis on hypothetical use cases is not a speculative exercise. Algorithmic systems are not only used for different purposes, they are used by different actors. Assessing a system's changing functionality without taking into account the wider context is futile, as a case involving the United Nations World Food Programme (WFP) illustrates.

In order to estimate need and distribute food aid, the WFP partners with local actors in conflict areas to enter biometric data of aid recipients into a database called SCOPE.[17] When the WFP announced a partnership with US data analytics and defense firm Palantir to streamline logistics,[18] Red Crescent workers on the ground in Syria raised serious concerns about their safety.[19] The association of WFP with Palantir,

---

[15] For a more detailed discussion of F-scores, see: https://deepai.org/machine-learning-glossary-and-terms/f-score

[16] For a conceptualization of dynamic functionality from a user perspective, see the work on affordances in ecological psychology such as: Rietveld, E., Denys, D., & Van Westen, M. (2018). Ecological-Enactive Cognition as Engaging with a Field of Relevant Affordances: The Skilled Intentionality Framework (SIF). In *Oxford Handbook for Embodied Cognitive Science*. Oxford University Press.

[17] For further reading about this case see Raftree, L. (2019). WFP-Palantir and the Ethics of Humanitarian Data Sharing. *Digital Impact*. https://digitalimpact.io/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing/

[18] Palantis is a software firm that develops applications used by military, intelligence agencies and police for big data analysis and predictive analytics.

[19] Red Crescent is a humanitarian organization and part of the International Red Cross and Red Crescent Movement: https://en.wikipedia.org/wiki/International_Red_Cross_and_Red_Crescent_Movement

known for its adherence to the US government and ties to the intelligence sector,[20] suggested the possibility of Syrian Red Crescent personnel supplying data to American agencies. As a result, Red Crescent workers feared retribution from the Assad government. Nevermind that Palantir did not have access to personal data,[21] a new potential use case caused the real possibility of lives being harmed.

Here, function creep does not involve a change in a data-processing system's proper activity. No actual algorithmic change had led to a new function. Nor did any legislative attempt at purpose limitation matter because there was no actual algorithmic activity. A new hypothetical function, an unrealised possibility for action, has placed the system and its stakeholders in a high-stakes web of geopolitics as well as situating it firmly in a history of technology-driven humanitarian and military interventions.

Creep is not Exceptional

Function creep is commonly declared to mark exceptions in a system that is otherwise functioning according to its specified purpose. It serves as a rhetorical device that signals control over a system's functionality, suggesting that the repurposing of a technology for unwanted ends is a technical shortcoming. Yet, cases such as the WFP-Palantir partnership testify to the limited information that algorithmic functionality offers when assessing the actions a system can be used for. In reality, algorithmic systems are sociotechnical apparatuses with a dynamic array of functions, the conditioning of which is an exercise of control. These systems cannot be understood in isolation but need to be read in relation to existing spheres of power, from the ideological to the algorithmic level.

Rhetorically limiting the flexible functionality of algorithmic systems serves to uphold social hierarchies. As Mbembe[22] puts it, technologies are increasingly tied in with complex networks of extraction and predation. It is this entanglement of algorithmic systems that drives the current fairness discourse in AI and it is from this context that rhetorical relapses into function creep need to be refuted. In these dominant narratives, exceptions are *creepy*, systems are distinct and change is controllable.

Function creep occurs when the use of an algorithmic systems deviates from what is considered its purpose. Dominant narratives and interests define what is considered a purpose, a correct use. These dominant stance is mirrored in operationalisations of human norms in ethical standards for algorithmic systems. For example, Sambasivan et al.point out that AI fairness is largely measured according to "Western concerns and histories - the structural injustices (e.g. race and gender), the data (e.g. ImageNet) [..] and enlightenment values".[23] When an AI system's performance is weighed in relation to its purpose, that process includes an array of assumptions about dominant norms.

Creep, a deviation from purpose, essentially serves as a pointer to how and with which norms a purpose is constructed. Discussions on creep thus imply the question who defines which norms form the baseline. Looking at how and when creep is signalled allows us to understand how norms are constructed. When function creep occurs and purpose limitation fails, it reveals who would (not) have been protected by the dominant norms governing an algorithmic system and its use.

---

[20] See for example Palantir's SEC Form S-1, filed ahead of its initial public offering in 2020: "*We have chosen sides*. Our software is used by the United States and its allies in Europe and around the world. Some companies work with the United States as well its adversaries. We do not. We believe that our government and commercial customers value this clarity." https://sec.report/Document/0001193125-20-230013/

[21] Palantir did not have access to SCOPE data according to WFP. But while personally identifiable data may not have directly been accessible to Palantir, logistics data may allow extrapolating demographically identifiable data and other group variables. See footnote 16 on WFP/Palantir and footnote 15 on group privacy.

[22] Mbembe, A. (2019). *Necropolitics*. Duke University Press Books.

[23] Sambasivan, N., Arnesen, E., Hutchinson, B., Doshi, T., & Prabhakaran, V. (2021). Re-imagining Algorithmic Fairness in India and Beyond. *ArXiv: 2101.09995 [Cs]*. http://arxiv.org/abs/2101.09995

The above implies that a different understanding of function creep is possible. Rather than understanding creep as a phenomenon that goes unnoticed until it appears, creep can be actively sought out to trace where and for whom a system fails. An example is provided by a study about a machine learning system that determines health risk scores in medical settings. Obermeyer et al. show that an algorithm for assigning risk scores to patients exhibits racial bias because it uses health costs as a substitute for health needs. [24] As a result, because less money is spent on patients who self-identify as black, they are assigned a lower risk score than white patients and thus are rated healthier than equally sick white patients. Crucially, the algorithm did not include race as a variable. The researchers inferred the variable, an action that was not built into the system but is a common method in statistical analysis. By repurposing the system, effectively using function creep, Obermeyer et al. were able to establish harmful effects of norms that were implicit in the algorithm's design.

Creep as Modus Operandi

While algorithmic systems are built to be repurposed,[25] the harmful effects of this openness are compartmentalized as aberrations from norms. In dominant narratives, function creep serves as a rhetorical device to mark routinely occurring deviations as anomalies. But function creep is not an exception, it is the modus operandi of any algorithmic system.

Actively leveraging function creep allows tracing the ongoing negotiation and erosion of the functionality of algorithmic systems, as well as the entanglement of algorithmic systems with networks of power and their stakeholders. The ideological and algorithmic frameworks of purpose limitation reveal who does (not) matter according to the norms governing and embedded in an algorithmic system. Function creep is a pointer to this conditionality of fairness.

~~**Addendum on next page**~~

---

[24] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

[25] In fact, creep and repurposing is what regularly drives research resulting in technological innovation. Take the 'creepy' work of Dina Katabi's team at MIT, who are using radio signals in the Wi-Fi frequency range to measure vital signs in retirement homes, "to detect outbreaks of infectious diseases like COVID-19". https://www.csail.mit.edu/news/home-health-device-uses-wireless-signals-identify-person-its-seen